View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

Europ. J. Combinatorics (1997) **18,** 11–33

Antipodal Distance-transitive Covers of Complete Bipartite Graphs

A. A. Ivanov, Robert A. Liebler, Tim Penttila and Cheryl E. Praeger

This paper completes the classification of antipodal distance-transitive covers of the complete bipartite graphs $K_{k,k}$, where $k \geqslant 3$. For such a cover the antipodal blocks must have size $r \leqslant k$. Although the case $r = k$ has already been considered, we give a unified treatment of $r \leqslant k$. We use deep group-theoretic results as well as representation-theoretic data about explicit linear groups and group coset geometries.

Apart from the generic examples arising from finite projective spaces, there are three sporadic examples (arising from the outer automorphisms of the symmetric group S_6 and of the Mathieu group M_{12} and one related to non-abelian Singer groups on $PG_2(4)$) and an infinite family having solvable automorphism group (and with parameters $r = q^b$, $k = q^a$, where $(q^b - 1)gcd(b, q-1)$ divides $2a(q-1)$ and q is a prime power).

© 1997 Academic Press Limited

1. Introduction

Let $\Gamma = (V, E)$ denote a finite, undirected, connected graph with vertex set V and edge set E. The *distance* $d(\alpha, \beta)$ between any $\alpha, \beta \in V$ is the length of the shortest path in Γ from α to β. The *diameter* d of Γ is the maximum distance between vertices of Γ. The graph Γ is said to be *distance-transitive* if its automorphism group $Aut\,\Gamma$ acts transitively on the set $\Gamma_i = \{(\alpha, \beta) \mid d(\alpha, \beta) = i\}$ of ordered pairs of vertices at distance i for all $0 \leqslant i \leqslant d$. In particular, a distance-transitive graph Γ is vertex-transitive, since $Aut\,\Gamma$ is transitive on Γ_0. In [23], D. H. Smith investigated finite connected distance-transitive graphs Γ for which $Aut\,\Gamma$ acts imprimitively on the vertex set V. The group $Aut\,\Gamma$ is said to be *imprimitive* on V if there is a partition Σ of V into blocks, each size r where $1 < r < |V|$, such that, for each $q \in Aut\,\Gamma$ and $B \in \Sigma$, the image $B^g \in \Sigma$. Smith [23] showed that there were only two types of partitions Σ which can be preserved by $Aut\,G$, for a finite imprimitive distance-transitive graph Γ of valency at least 3, namely:

(1) $\Sigma = \{\Delta_1, \Delta_2\}$, and each edge of Γ joins a vertex of Δ_1 to a vertex of Δ_2, in which case Γ is *bipartite*; and

(2) $\Sigma = \{\{\alpha\} \cup \Gamma_d(\alpha) \mid \alpha \in V\}$, in which case Γ is *antipodal.*

Here we use the notation $\Gamma_i(\alpha) = \{\beta \mid (\alpha, \beta) \in \Gamma_i\}$ for $0 \leqslant i \leqslant d$. In general, a graph Γ is said to be *antipodal* if the collection of sets $\{\{\alpha\} \cup \Gamma_d(\alpha) \mid \alpha \in V\}$ forms a partition of V, which is then called the *antipodal partition* of V. With any antipodal graph Γ we can associate a natural *quotient* graph, which we shall denote by Γ', the vertex set of which is the antipodal partition of Γ, two antipodal blocks being adjacent in Γ' whenever they contain adjacent vertices of Γ. If Γ is antipodal and its antipodal blocks have size r, then Γ is called an *r-fold antipodal cover* of Γ'. Smith [23] showed, moreover, that if Γ is a finite antipodal distance-transitive graph then its antipodal quotient Γ' is also distance-transitive. Thus, as part of the problem of classifying finite distance-transitive graphs, all distance-transitive, antipodal covers of the known distance-transitive graphs must be determined. This has been done by J. van Bon and A. E. Brouwer [2] for most of the known families of finite distance-transitive graphs in which the diameter is unbounded.

0195-6698/97/010011 + 23 $25.00/0 ej930086 © 1997 Academic Press Limited

The complete bipartite graph $K_{k,k}$ is distance-transitive and antipodal distance-transitive covers of $K_{k,k}$ occur as extreme examples of antipodal distance-transitive graphs: in [13, Corollary 4.4 and Proposition 4.6] A. Gardiner showed that, for a distance-transitive r-fold antipodal cover of a graph Γ of valency $k \geqslant 3$ to exist, the index r is at most k, and if $r = k$, then either $k = 3$ and Γ is Tutte's eight-cage, or $k = 6$, $\Gamma' = K_7$ and Γ is the subgraph induced on the vertices at distance 2 from a given vertex in the Hoffman–Singleton graph, or $\Gamma' = K_{k,k}$. In further work Gardiner [14] showed that a distance-regular k-fold antipodal cover of $K_{k,k}$ is the incidence graph of the design of points and lines of some affine plane of order k with one parallel class of lines omitted. Earlier, A. Cronheim [8] had studied just this geometric configuration as a generalization of the abstract Pappus configuration ($k = 3$). Cronheim showed that this incidence system arises as a coset geometry within the group of (∞, ∞)-perspectivities whenever the associated projective plane is in Lenz class V or greater (so called semifield planes).

Gardiner observed that when the above construction is applied to the Desarguesian affine plane or order k one obtains an example of a distance-transitive k-fold antipodal cover of $K_{k,k}$. Gardiner further observed that the incidence graph arising from the above construction is distance-transitive whenever the associated projective plane is self-dual and the affine plane admits a rank 3 permutation group on its points. This is exactly the sitution left by earlier authors but handled in [19]. The associated plane is in Lenz class V and Cronheim's coset geometry construction applies. The twisted field planes of Albert [1] appear as the only known rank 3 affine semifield planes in the survey [17]. Chuvaeva and Pasechnik [6] rediscovered all of this and repeated Albert's characterization of the self-dual twisted field planes. In [20, Theorem 3.6] Cronheim's coset geometry is used to give a representation-theoretic characterization of some generalized twisted field planes (including those that are rank 3). More recently, the classification of finite simple groups has allowed the extension of this argument [21] to a classification of distance-transitive k-fold antipodal covers of $K_{k,k}$.

It turns out that r-fold antipodal distance-transitive covers of $K_{k,k}$ arise in three ways: first, as the opposites to a fixed flag in the symmetric design D of points and hyperplanes associated with a finite projective geometry—Construction 1.1; second, as certain points and hyperplanes off a fixed antiflag in D—Construction 1.2; and, finally, as bi-additive forms that are equivariant under transitive linear groups—Constructions 5.7 and 6.2.

Construction 1.1 is a natural generalization of Gardiner's construction. It requires the followng definition. Suppose that D is the symmetric design of points and hyperplanes associated with a finite projective geometry and let (w, H) be an incident point, hyperplane pair (or *flag*) in D. Let $\Delta^{(1)}$ denote the set of all points not in H and let $\Delta^{(2)}$ denote the set of all hyperplanes not containing w. Then $\mathsf{D}^{op(w,H)}$ is defined to be the incidence structure ($\Delta^{(1)}$, $\Delta^{(2)}$, incidence of D) and is called the *opposites to* (w, H) *in* D; it is often written more simply as D^{op} when the pair (w, H) is obvious from the context. We also abuse notation and use D^{op} to denote the incidence graph of this incidence structure when no confusion arises.

CONSTRUCTION 1.1. *Let $PG_n(q)$ be the design of* 1*-dimensional and n-dimensional subspaces of an $(n+1)$-dimensional vector space W over $GF(q)$. Then the incidence graph of the opposites to (w, H) is distance-regular. Each antipodal block in $\Delta^{(1)}$ is the set of points (apart from w) of a fixed* 2*-dimensional subspace on w and each antipodal block in $\Delta^{(2)}$ is the set of hyperplanes (apart from H) containing a fixed $(n-1)$-dimensional subspace of H.*

The group $Aut\, PG_n(q)^{op}$ has a subgroup of index $2\,|Aut\, GF(q)|$ that consists of block *triangular matrices with blocks of size* $1, n-1, 1$ *relative to an appropriate basis of W, as described in the penultimate paragraph of Section* 4. $PG_n(q)^{op}$ *is a distance-transitive q-fold antipodal cover of* $K_{q^{n-1},q^{n-1}}$.

Let Π *be a non-Desarguesian projective plane of order* q^n. *Then* Π^{op} *is a distance-regular* q^n*-fold cover of* K_{q^n,q^n}, *as mentioned above and observed by Gardiner.*

Suppose that Π *is self-dual, in Lenz class V with distinguished flag* (∞, l_∞) *and of dimension r over its kern* $GF(q)$; *see* [10, *Section* 5.2] *for definitions. If, further more,* Π *meets Gardiner's criterion that the associated affine plane admits a rank* 3 *permutation group on its points, then* $\Pi^{op(\infty,l_\infty)}$ (*has an incidence graph that*) *is distance-trasitive.*

As already mentioned, Chuvaeva and Pasechnik [6] observed that certain planes Π cordinatized by the twisted fields of Albert meet the criterion of the final paragraph above (see also our Construction 5.6). In this case it turns out that $Aut\,\Pi^{op}$ has a subgroup H of index dividing $2\,|Aut\,GF(q)|$ and a normal subgroup P of order q^{3n} such that $|H/P| = (q^n-1)(q-1)$.

At the heart of the longest part of our argument lies the coset geometry construction of Cronheim that leads (see Lemma 4.4) to a transformation of these graphs (together with their classification problem) to the third view mentioned above, namely to certain bi-additive equivariant forms. The above geometric constructions are transformed to their equivariant forms at the end of Section 4 in the proof of Lemma 4.6 and the note following; and in Construction 5.6.

Two sporadic constructions rely on exceptional properties of the symmetric group S_6 with $\mathsf{D} = PG_3(4)$ and the Mathieu group M_{12} with $\mathsf{D} = PG_6(3)$. In each case the indicated group possesses a (projective) representation as a collineation group of D fixing a non-incident point, hyperplane pair (w, H) and the only other (projective) representation of the same dimension over the indicated field is the contragredient of the first. In each case there are point and hyperplane orbits $\Delta^{(1)}$ and $\Delta^{(2)}$ such that (the incidence graph of) ($\Delta^{(1)}$, $\Delta^{(2)}$, incidence of D) is a distance-transitive cover of a complete bipartite graph. This complete bipartite graph has the elements of certain point and hyperplane orbits O and E within the hyperplane H 'at infinity' as its vertices. Thus each antipodal block in $\Delta^{(1)}$ is the set of points (apart from w, a) of a line $\langle w, a\rangle$ on w that meets H in some fixed $a \in \mathsf{O}$. And each antipodal block in $\Delta^{(2)}$ is the set of hyperplanes (apart from H, $\langle e, w\rangle$) containing a fixed $e \in \mathsf{E}$ (here we merely present the construction without verifying transitivity).

CONSTRUCTION 1.2. *In the case of* S_6, *the points and lines of H each fall into two orbits of sizes* 6 *and* 15. *The short point orbit* O *forms a hyperoval and the short line orbit* E *forms the set of exterior* (*incident with no element of* O) *lines to* O. *The set* $\Delta^{(1)}$ *is the set of all points on lines* $\langle w, a\rangle$ *other than w or a, for* $a \in \mathsf{O}$ *and the set* $\Delta^{(2)}$ *is the set of all planes on e other than H and* $\langle e, w\rangle$, *for* $e \in \mathsf{E}$.

In the case of M_{12}, *we recall the construction of the ternary Golay code. Label the elements of the* 12*-set upon which* M_{12} *acts with the points of an extended Paley Hadamard design* H *or order* 3 *in such a way that Aut* $\mathsf{H} = M_{12}$ [3, *p.* 227]. *Because the incidence matrix of* H *modulo* 3 *has rank* 6, *the blocks of* H *span a* 6*-dimensional* $GF(3)$*-vector space A which is the ternary Golay code. View A as an affine space and embed it in a projective space* $PG(6, 3)$, *taking H to be the hyperplane* '*at infinity*', *and take w to be the zero element of A.*

Now the points and 4*-flats of H each fall into three* M_{12}*-orbits of sizes* 12, 132 *and* 220 [24]. *Moreover, the short point orbit* O *arises from the blocks of* H *as above and the short* 4*-flat orbit* E *is the set of exterior* 4*-flats to* O [24]. *The set* $\Delta^{(1)}$ *is the set of all points on lines* $\langle w, a\rangle$ *other than w or a, for* $a \in \mathsf{O}$ *and the set* $\Delta^{(2)}$ *is the set of all hyperplanes on e other than H and* $\langle e, w\rangle$, *for* $e \in \mathsf{E}$.

Incidently, the above S_6 construction with point and line orbits of size 15 in place of 6 gives a geometric construction of the 3-fold cover of the generalized quadrangle of order $(2, 2)$ described as Tutte's eight-cage above. This graph plays an important role in the 'geometrization' of sporadic finite simple group constructions.

In addition to the above examples, we have found another sporadic example and an infinite family of distance-transitive covers of complete bipartite graphs that are apparently new. We describe them as equivariant forms only and therefore postpone their introduction until this machinery is developed. They appear in Constructions 5.7 and 6.2, respectively. The second part of Construction 1.1 is described as an equivariant form in Construction 5.6. The main purpose of this paper is to establish the following:

MAIN THEOREM. *Let Γ be a distance-transitive r-fold antipodal cover Γ of $K_{k,k}$. Then one of the following holds:*
(1) *Γ is the incidence graph of $PG_n(r)^{op}$, for some $n \geqslant 2$ and $k = r^{n-1}$.*
(2) *Γ is the incidence graph of $\Pi^{op(\infty, l_\infty)}$, where Π is a self-dual twisted field plane and $k = r$.*
(3) *$\Gamma = 3.K_{6,6}$, and $Aut\,\Gamma = 3 \cdot Aut\, S_6$.*
(4) *$\Gamma = 2.K_{12,12}$ is a Hadamard graph and $Aut\,\Gamma = 2 \cdot Aut\, M_{12}$.*
(5) *Γ has parameters $r = q^b$, $k = q^a$, where $(q^b - 1)gcd(b, q-1)$ divides $2a(q-1)$ and $q = p^c$ is a prime power, and $Aut\,\Gamma \geqslant p^{bc} \cdot p^{2ac} \cdot GL(1, q^a) \cdot (q^b - 1) \cdot 2$.*
(6) *$\Gamma = 8.K_{64,64}$ and $|Aut\,\Gamma| = 2^3 \cdot 2^{12} \cdot 3 \cdot 7 \cdot 3 \cdot 2$.*

It must be pointed out that our argument depends essentially on the classification of finite simple groups via the proof of the Schreier conjecture and the classification of 2-transitive groups [5]. It breaks into two, essentially group-theoretic, cases. The almost simple case appears in Section 3 and leads to the sporadic examples given in Construction 1.2, while the affine case leads to a coset geometry construction and commutator maps in special p-groups [8] in Section 4. These maps are then interpreted as bi-additive equivariant forms and those that are invariant under Singer cycles are studied in Section 5. Also, the examples arising in cases 2 and 6 of the Main Theorem are also presented as equivariant forms in this section. The treatment of the affine case is completed in Section 6. The final section also contains Theorem 6.5, which fills a small gap in [21] by strengthening [20, 3.6].

Much of this argument does not require the full 'distance-transitive' hypothesis. For example, Corollary 5.3 applies to any distance-regular antipodal cover of a complete bipartite graph possessing a 'T-group' in the sense of Cronheim (cf. Lemma 4.3) and a collineation of $(k-1)$-primitive prime divisor order.

2. Basic Notation

Let $\Gamma = (V, E)$ be a finite connected graph which is a distance-transitive r-fold antipodal cover of $\Gamma' = K_{k,k}$. From [13, Proposition 5.9] we have the following information about Γ. The diameter d of Γ is 4 and, for $\alpha \in V$, the sets $\Gamma_i(\alpha)$ of vertices at distance i from α satisfy

$$|\Gamma_1(\alpha)| = k, \qquad |\Gamma_2(\alpha)| = (k-1)r, \qquad |\Gamma_3(\alpha)| = k(r-1), \qquad |\Gamma_4(\alpha)| = r-1.$$

For a distance-transitive graph Γ of diameter 4, the *intersection array* of Γ is defined as $i(\Gamma) = \{b_0, b_1, b_2, b_3;\ c_1, c_2, c_3, c_4\}$, where for $\beta \in \Gamma_i(\alpha)$, $b_i = |\Gamma_1(\beta) \cap \Gamma_{i+1}(\alpha)|$ and $c_i = |\Gamma_1(\beta) \cap \Gamma_{i-1}(\alpha)|$. For our graph Γ, the intersection array, by [14], is

$$i(\Gamma) = \{k, (k-1), k(r-1)/r, 1; 1, k/r, (k-1), k\}.$$

The graph Γ is both bipartite and antipodal. Let $\{\Delta^{(1)}, \Delta^{(2)}\}$ be the bipartition of V, and let $\Sigma = \{B_1^{(1)}, \ldots, B_k^{(1)}, B_1^{(2)}, \ldots, B_k^{(2)}\}$ be the antipodal partition of V, where $\Delta^{(i)} = \bigcup_{1 \leqslant j \leqslant k} B_j^{(i)}$ for $i = 1, 2$. We call elements of $\Delta^{(i)}$ vertices of *type i.* Set $\Sigma^{(i)} = \{B_1^{(i)}, \ldots, B_k^{(i)}\}$, the set of antipodal blocks in $\Delta^{(i)}$ for $i = 1, 2$. Then $\{\Sigma^{(1)}, \Sigma^{(2)}\}$ is the bipartition of the vertex set Σ of the antipodal quotient $\Gamma' = K_{k,k}$.

We also use the incidence system $(\Delta^{(1)}, \Delta^{(2)}, E)$ having as *points* the vertices of type 1, as *lines* the vertices of type 2 and as *flags* the edges E of Γ. Call the elements of $\Sigma^{(1)}$ *blocks* and the elements of $\Sigma^{(2)}$ *parallel classes.*

Lemma 2.1. (1) *Each line (point) is incident with k points (lines).*
(2) *Each block (parallel class) contains r points (lines).*
(3) *The blocks (parallel classes) partition the points (lines).*
(4) *Any two points not in the same block (non-parallel lines) share k/r lines (points).*
(5) *Each line (point) is incident with exactly one point (line) from each block (parallel class).*
(6) *When $r = k$, the incidence structure of points versus lines $\cup$ blocks is an affine plane of order k.*

Proof. The first four claims are restatements of the parameters of Γ. The fifth claim follows from the third and the fact that the antipodal quotient of Γ is bipartite, and the final claim follows from the others.

Let $G \leqslant Aut\,\Gamma$ be any subgroup of automorphisms of Γ which is distance-transitive on Γ; that is, G is transitive on Γ_i for $0 \leqslant i \leqslant 4$. As well as being antipodal, the graph Γ is bipartite. Let G^+ be the subgroup of index 2 in G which fixes $\Delta^{(1)}$ and $\Delta^{(2)}$ setwise, so that G^+ is an automorphism group of the incidence structure defined before Lemma 2.1.

Let $H^{(i)}$ be the permutation group induced by G^+ on $\Sigma^{(i)}$, the set of blocks for $i = 1$ (set of parallel classes for $i = 2$). Let $K^{(i)}$ be the subgroup of G^+ which fixes each $B_j^{(i)}$, $j = 1, \ldots, k$ setwise. Thus $K^{(1)}$ ($K^{(2)}$) is the largest subgroup of G^+ acting trivially on the set of blocks (parallel classes). Then $H^{(i)} \simeq G^+/K^{(i)}$, for $i = 1, 2$.

Let $K = K^{(1)} \cap K^{(2)}$ be the (normal) subgroup of G which fixes each $B_j^{(i)}$ setwise, and hence acts trivially on the set of blocks and the set of parallel classes. (In case $k = r$, K is the group of (∞, l_∞)-perspectivities of the associated projective plane.)

Let $G_{(B)}$ denote the pointwise stabilizer of $B \in \Sigma$ in G. Then the permutation group $L = G_B/G_{(B)}$ induced by G_B on B does not depend on the choice of B, in view of the transitivity of G on Σ.

The following lemma gives some significant information about the structure of G.

Lemma 2.2. (1) *The group $H^{(i)}$ is 2-transitive of degree $|\Sigma^{(i)}| = k$, for $i = 1, 2$.*
(2) *The group G^+ is transitive on the Cartesian product $\Sigma^{(1)} \times \Sigma^{(2)}$; the actions of G^+ on $\Sigma^{(1)}$ and $\Sigma^{(2)}$ are not permutationally isomorphic, but conjugate in G.*
(3) *The permutation group L is 2-transitive of degree r.*
(4) *If $K \neq 1$, it is elementary abelian of order $r = p^b$, for some prime p and integer $b \geqslant 1$ and K acts regularly—that is, faithfully and transitively—on each $B \in \Sigma$.*

Proof. Let $\alpha \in B$ for $B = B_1^{(1)} \in \Sigma^{(1)}$. Since G is transitive on the vertex set V, G^+ is transitive on $\Gamma_i(\alpha)$ for $i = 1, 2, 3, 4$. By Lemma 2.1.4, $\Gamma_1(\alpha)$ contains one point from each block $B_j^{(2)}$ of $\Sigma^{(2)}$, so G_α and hence G_B is transitive on the set $\Sigma^{(2)}$ of parallel classes. Thus G^+ is transitive on $\Sigma^{(1)} \times \Sigma^{(2)}$. Claim (2) follows from the transitivity of G on V.

Since $\Gamma_2(\alpha)$ is the union $\bigcup_{2\leqslant j\leqslant k} B_j^{(1)}$, it follows that G_α and hence G_B is transitive on $\Sigma^{(1)}\setminus\{B_1^{(1)}\}$. Thus G^+ is 2-transitive on $\Sigma^{(1)}$ and, similarly, G^+ is 2-transitive on $\Sigma^{(2)}$. Now Claim (1) follows. Since $B=\{\alpha\}\cup\Gamma_4(\alpha)$ and G_α is transitive on $\Gamma_4(\alpha)$, it follows that G_B is 2-transitive on B, and Claim (3) follows.

Now suppose that $K\neq 1$. Then the permutation group K^B induced by K on B is a non-trivial normal subgroup of $L=G_B^B$. Since L is 2-transitive, it follows that K^B is transitive. Now K_α fixes $B_j^{(2)}\cap\Gamma_1(\alpha)$ setwise (a set of size 1) for each $j=1,\dots,k$, and hence K_α fixes $\Gamma_1(\alpha)$ pointwise. Let $\beta\in\Gamma_1(\alpha)$. Then $K_\alpha=K_\beta$ fixes $\Gamma_1(\beta)$ pointwise, and so on. Since Γ is connected it follows that $K_\alpha=1$. Thus K acts regularly on B and, consequently, K is elementary abelian of order r (see [4, Section 154]).

It was further proved by Burnside [4, Section 154] that a finite 2-transitive group H is either *almost simple* (that is, $T\leqslant H\leqslant Aut\,T$ for some non-abelian simple group T) or is *affine* (that is, $H\leqslant AGL_a(p)$ for some prime p and integer $a\geqslant 1$ and H contains every translation). By Lemma 2.2.1, $H^{(1)}$ and $H^{(2)}$ are both almost simple, or are both affine. We shall treat these cases separately. In the next section we deal with the case in which $H^{(1)}$ and $H^{(2)}$ are almost simple, and beginning in Section 4 we consider the case in which they are both affine.

3. The Almost Simple Case

We use the notations and assumptions of the previous section, and in addition assume that, for $i=1,2$, $T\leqslant H^{(i)}\leqslant Aut\,T$ for some non-abelian simple group T. Our treatment in this section relies on the classification of finite simple groups: we use both the classification of the finite almost simple 2-transitive permutation groups and the 'Schreier conjecture' that the outer automorphism group of a finite simple group is soluble [5].

Lemma 3.1. *One of the following holds:*
(1) *for* $i=1,2$, $K^{(i)}\neq K$;
(2) $\Gamma=3\cdot K_{6,6}$, $G=3\cdot Aut\,S_6$, $k=6$, $r=3$;
(3) $\Gamma=2\cdot K_{12,12}$, $G=2\cdot Aut\,M_{12}$, $k=12$, $r=2$.

Proof. Suppose that $K^{(i)}=K$ for some i. Then, by Lemma 2.2, $K=K^{(1)}=K^{(2)}$ and G^+/K acts faithfully and 2-transitively on $\Sigma^{(1)}$ and $\Sigma^{(2)}$. Moreover, these actions are not equivalent but are interchanged by (any) $g\in G\setminus G^+$. In fact, G^+/K is transitive on $\Sigma^{(1)}\times\Sigma^{(2)}$. The almost simple 2-transitive groups have been classified and are listed in [5]. The only ones which have two 2-transitive representations, on $\Sigma^{(1)}$ and $\Sigma^{(2)}$, and are transitive on $\Sigma^{(1)}\times\Sigma^{(2)}$, are A_6 or S_6 of degree $k=6$, and M_{12} of degree $k=12$. The distance-transitive graphs of valencies 6 and 12 have been classified in [12] and [16] (see also [15] and [3]) and it follows that Γ is as given in the lemma. □

Assume that $K^{(i)}>K$ for $i=1,2$. Therefore G^+ has a normal subgroup $T^{(i)}$ such that $K<T^{(i)}\leqslant K^{(i)}$ and $T^{(i)}/K\simeq T$, for $i=1,2$, and $T^{(1)}\cap T^{(2)}=K$. Next, we investigate the action of $K^{(i)}$.

Lemma 3.2. *For* $i=1,2$ *and* $j=1,\dots,k$, *the pointwise stabilizer of* $B_j^{(i)}$ *in* $K^{(i)}$ *is trivial.*

Proof. Suppose that the subgroup $N^{(1)}$ of $K^{(1)}$ fixing $B_1^{(1)}$ pointwise is non-trivial. By Lemma 2.2.4, $N^{(1)}$ is not contained in K, and so $N^{(1)}$ acts non-trivially on $\Sigma^{(2)}$. Thus

$N^{(1)}K^{(2)}/K^{(2)}$ is a non-trivial subnormal subgroup of $G^+/K^{(2)} = H^{(2)}$, and so $N^{(1)}K^{(2)}/K^{(2)} \geqslant T$, whence $N^{(1)}/(N^{(1)} \cap K^{(2)}) \geqslant T$. Furthermore $N^{(1)} \cap K^{(2)} = N^{(1)} \cap K$, and by Lemma 2.2.4 this group is trivial, so $N^{(1)}$ acts faithfully on $\Sigma^{(2)}$. Thus $N^{(1)}$ has a normal subgroup M isomorphic to T. Now $N^{(1)}$ and K are normal subgroups of $K^{(1)}$ and $N^{(1)} \cap K = 1$, so $N^{(1)} \times K \leqslant K^{(1)}$. Moreover, since $Aut\, T \geqslant K^{(1)}K^{(2)}/K^{(2)} \geqslant N^{(1)}K^{(2)}/K^{(2)} \geqslant T$ and $Aut\, T/T$ is soluble by the 'Schreier conjecture', and since $K^{(1)} \cap K^{(2)} = K$ and K is abelian, it follows that $K^{(1)}/M$ is soluble. Thus M is the last term in the derived series for $K^{(1)}$, so that M is a characteristic subgroup of $K^{(1)}$, and hence M is normal in G^+. Since M fixes $B_1^{(1)}$ pointwise, it follows that M fixes $\Delta^{(1)}$ pointwise.

Let $g \in G \setminus G^+$. Then M^g fixes $\Delta^{(2)}$ linewise and so $M \cap M^g = 1$. Thus $M \times M^g = \langle M, M^g \rangle$ is a normal subgroup of G and the set of orbits of $M \times M^g$ in V is a G-invariant partition of V. This partition is not the antipodal partition, since M is transitive on $\Sigma^{(2)}$ and hence, by [23], it must be the bipartition $\{\Delta^{(1)}, \Delta^{(2)}\}$ of V. This implies that M is transitive on $\Delta^{(2)}$, which is not the case since M fixes $\Gamma_1(\alpha)$ setwise. □

LEMMA 3.3. *The only r-fold antipodal distance-transitive covers of $K_{k,k}$ with $r < k$ and with the groups $H^{(i)}$ almost simple are the two examples obtained in Lemma* 3.1.

PROOF. Let $G_{(B)}$ denote the pointwise stabilizer of $B = B_1^{(1)}$ in G. Then $G_B^B = G_B/G_{(B)}$, the permutation group induced by G_B on B, has a normal subgroup $K^{(1)}G_{(B)}/G_{(B)}$ which, by Lemma 3.2, is isomorphic to $K^{(1)}$. If $K \neq 1$ then, by Lemma 2.2, K is transitive on B and $K_\alpha^{(1)}$, for $\alpha \in B$, is isomorphic to $K^{(1)}/K$; $K^{(1)}/K$ has a subgroup $T^{(1)}/K \simeq T$ which is normalized by G^+/K. Furthermore, if $K \neq 1$, then K is regular on B of prime power degree $|B| = r = p^b$ by Lemma 2.2.4, and hence $K_\alpha^{(1)}$, for $\alpha \in B$, acts faithfully on $\Sigma^{(2)}$. Thus $K_\alpha^{(1)} \simeq (K_\alpha^{(1)})^{\Sigma^{(2)}} = (K_\alpha^{(1)}K)^{\Sigma^{(2)}} = (K^{(1)})^{\Sigma^{(2)}}$ which has socle isomorphic to T. Since $K_\alpha^{(1)}$ acts faithfully on B (by Lemma 3.2) and is normal in G_α, it follows that T is isomorphic to a normal subgroup of $(G_\alpha)^B \leqslant Sym(B)$. Then, since G_α is transitive on $B \setminus \{\alpha\}$, the T-orbits in $B \setminus \{\alpha\}$ have equal length s, say, where $s > 1$ and s divides $r - 1$. On the other hand, if $K = 1$, then $T \simeq T^{(1)}$ is the socle of $K^{(1)} \simeq (K^{(1)})^{\Sigma^{(2)}}$. Again, since $K^{(1)}$ is faithful on B (by Lemma 3.2) and is normal in G_B, T is isomorphic to a normal subgroup of the 2-transitive group G_B^B, and hence T is transitive on B of degree r. Thus we have shown that T has a proper subgroup of index s, where either $s = r$, or r is a prime power and s divides $r - 1$. Recall that r is a proper divisor of K.

The list of almost simple 2-transitive groups of degree k is given in [5]. In no case does the socle T of one of these groups have a proper subgroup of index a proper divisor of k, or of index dividing $r - 1$, where $r = p^b$ is a proper divisor of k. □

4. THE COSET GEOMETRY

We use the notation and assumptions of Section 2, and in addition assume that, for $i = 1, 2$, $H^{(i)} \leqslant AGL(a, p)$ for some prime p and some integer $a \geqslant 1$, and so H contains every translation. So $k = p^a$. In this section we show in Lemma 4.4 that Γ may be reconstructed from a coset geometry in the sense of Tits [10, 1.2.17] in a p-group P. The group P is special and acts regularly on the edges E of Γ and, consequently, the coset geometry is determined by the commutator map of P together with its subgroups P_α and P_β for $(\alpha, \beta) \in E$ (Lemma 4.4) in a way first studied by Cronheim [8].

In the generic case in which $\Gamma = PG_n(q)^{op}$ is the incidence graph of opposites to the incident point hyperplane pair (w, H) in $PG_n(q)$, cf. Construction 1.1, the group P is generated by all transvections with center w or axis H and is also equal to the kernel of the action of $PGL(n+1, q)_{wH}$ on the quotient space H/w. This is also the largest normal p-subgroup of G^+.

The first step is to construct the special group P. We begin by showing that the group $K = G_{(\Sigma)}$ leaving invariant each block and each parallel class is non-trivial.

Lemma 4.1. *The subgroup K is elementary abelian of order $r = p^b$ and acts regularly on each block $B_j^{(i)}$ in Σ.*

Proof. As r divides k, $r = p^b$ for some b. If $K \neq 1$, then Lemma 2.2.4 implies that K is elementary abelian of order $r = p^b$ and is regular on each $B_j^{(i)}$. Suppose that $K = 1$ and set $Q = O_p(G^+)$, where $O_p(G)$ is the largest normal p-subgroup of G. Then $Q \neq 1$, since G^+ acts faithfully on Σ, and $H^{(i)} = (G^+)^{\Sigma^{(i)}} \leqslant AGL(a, p)$ and is 2-transitive. Also, $Q \simeq Q^{\Sigma} \leqslant Q^{\Sigma^{(1)}} \times Q^{\Sigma^{(2)}}$, and so Q is elementary abelian of order at most p^{2a}. Now the orbits of Q are blocks of imprimitivity for G in V, so by the result of D. H. Smith stated in Section 1, Q is transitive on $\Delta^{(i)}$, $i = 1, 2$. As Q is abelian, Q is regular on $\Delta^{(1)}$, and the subgroup $Q_1 = Q_{(\Delta^{(1)})}$ of Q fixing $\Delta^{(1)}$ pointwise is normal in G^+ and hence is either transitive, and hence regular, or trivial on $\Sigma^{(2)}$. Since Q acts faithfully on Σ, $Q_1 \simeq Q_1^{\Sigma^{(2)}}$ has order 1 or p^a, whence $|Q| = |Q^{\Delta^{(1)}}|\,|Q_1|$ is either $|\Delta^{(1)}| = rk = p^{a+b}$, or $|\Delta^{(1)}| \cdot p^a = p^{2a+b}$. Since $|Q| \leqslant p^{2a}$ it follows that $Q_1 = 1$ and $|Q| = p^{a+b}$. Let $R = Q_{(\Sigma^{(1)})} = Q \cap K^{(1)}$. Then $|Q\colon R| = p^a$ and so $|R| = p^b$. Since R is faithful on Σ, $R^{\Sigma^{(2)}} \simeq R$ is a non-trivial normal subgroup of the 2-transitive group $H^{(2)}$ and so $R^{\Sigma^{(2)}}$ is transitive. Hence $|R| \geqslant p^a$ implies that $b = a$.

Now Lemma 2.1.6 implies that R acts trivially on the parallel class of the associated affine plane that we call blocks. Pick non-trivial $x \in R$. Then x is a central collineation of the associated projective plane and so it must also be axial [10, 1.4.8, 1.4.9]. This means that x must fix exactly one block, say $B_1^{(1)}$ pointwise. But Q is abelian and must therefore leave $B_1^{(1)}$ invariant, contrary to the fact that Q acts transitively on $\Sigma^{(1)}$. □

Next we deal with the possibility that $K^{(1)} = K^{(2)} = K$.

Lemma 4.2. *If $K^{(1)} = K$, then $k = 8$, $r = 2$ and case* (1) *of the Main Theorem holds.*

Proof. If $K^{(1)} = K$, then $K^{(1)}$ is normal in G and also $K^{(2)} = K$, so G^+/K acts faithfully on $\Sigma^{(1)}$. Let Q be $O_p(G^+)$. Then $K \leqslant Q$ by Lemma 4.1 and $Q/K \simeq Q^{\Sigma^{(1)}} \simeq Z_p^a$, so $|Q| = p^{a+b}$. It follows that Q is regular on $\Delta^{(i)}$ for $i = 1, 2$. Let $B = B_1^{(1)}$ and $\alpha \in B$. Then $G^+ = QG_\alpha$, $H^{(1)} = G^+/K \simeq (Q/K) \cdot G_\alpha$ and $G_B = KG_\alpha$, whence G_α is transitive on $\Sigma^{(1)} \setminus \{B\}$ and $G_\alpha \simeq G_\alpha^{\Sigma^{(1)}} \leqslant GL(a, p)$. Also, G_α is transitive on $\Gamma_1(\alpha)$ and hence G_α is transitive on $\Sigma^{(2)}$. Since $(G^+)^{\Sigma^{(2)}}$ is 2-transitive, $(G^+)_{B_1^{(2)}}$ is transitive on $\Sigma^{(2)} \setminus \{B_1^{(2)}\}$ of degree $p^a - 1$, and $(G_\alpha)_{B_1^{(2)}}$ is a subgroup of $(G^+)_{B_1^{(2)}}$ of index p^a, relatively prime to $p^a - 1$. It follows that $(G_\alpha)_{B_1^{(2)}}$ is also transitive on $\Sigma^{(2)} \setminus \{B_1^{(2)}\}$; that is, G_α is 2-transitive on $\Sigma^{(2)}$. Thus we have G_α acting faithfully and 2-transitively on $\Sigma^{(2)}$, properly contained in the affine 2-transitive group $H^{(2)}$; it follows from [22, Proposition 5.2] that $G_\alpha^{\Sigma^{(2)}} \geqslant GL(3, 2)\ wr\ S_l$, in product action if $l \geqslant 2$, $H^{(2)} \leqslant AGL(3, 2)\ wr\ S_l$ and $k = p^a = 8^l \geqslant 8$. Since $G_\alpha^{\Sigma^{(2)}}$ is 2-transitive we must have $l = 1$, so $k = 8$, r is 2 or 4 and $G_\alpha = GL(3, 2)$. But G_α also acts transitively on $B \setminus \{\alpha\}$ by Lemma 2.2.3, and so has a subgroup of index $r - 1$. Therefore $r = 2$. The distance-transitive graphs of valency 8 are classified in [16] (cf. [3, 7.5.2, 7.5.3(v)]), and there is only one with these parameters, namely $PG_2(2)^{op}$. □

Now assume that $K^{(2)} \neq K$ or, equivalently, that $K^{(1)} \neq K$. By assumption, the group

$(K^{(2)})^{\Sigma^{(1)}}$ induced by $K^{(2)}$ on the blocks is a non-trivial normal subgroup of the affine 2-transitive group $H^{(1)}$ acting on blocks, so $(K^{(2)})^{\Sigma^{(1)}}$ contains the full translation subgroup $T^{(1)}$ of $H^{(1)}$. Define a subgroup P_2 by $K \leqslant P_2 \leqslant K^{(2)}$, and $P_2/K \simeq P_2^{\Sigma^{(1)}} = T^{(1)}$. Similarly, define P_1 by $K \leqslant P_1 \leqslant K^{(1)}$, and $P_1/K \simeq P_1^{\Sigma^{(2)}} = T^{(2)}$, where $T^{(2)}$ is the full translation subgroup of $H^{(2)}$.

LEMMA 4.3. *Let $(\alpha, \beta) \in E$ be an incident (point, line) pair with $\alpha \in \Delta^{(1)}$ and $\beta \in \Delta^{(2)}$, and define groups $Q_1 = P_{1\,\alpha}$ and $Q_2 = P_{2\,\beta}$. Then:*
(1) *The group $K = P_1 \cap P_2$.*
(2) *The group $P_2 = Q_2 \times K$ ($P_1 = Q_1 \times K$) is elementaty abelian and acts regularly on points (lines).*
(3) *$P = P_1P_2 = Q_1KQ_2$ is normal in G and acts regularly on E. Moreover, $K \leqslant Z(P)$.*

PROOF. The first claim is immediate from the regularity of P_2/K on $\Sigma^{(1)}$. By Lemma 4.1, and the definition of P_i, P_i acts regularly on $\Delta^{(3-i)}$ and, for example, $P_2 = KQ_2$ has order kr.

Let $\Pi \in \Sigma^{(2)}$ be the parallel class of β. Since K acts transitively on Π by Lemma 2.1.5, the kernel S of the action of P_2 on Π has order less than or equal to $|P_2|/|K| = k$. By the preceding paragraph, S acts faithfully as a normal subgroup of the 2-transitive group $H^{(1)}$ that G^+ induces on the blocks $\Sigma^{(1)}$. If $|S| < k$, then S acts trivially on $\Sigma^{(1)}$, contrary to Lemma 2.1.5. Therefore $S = Q_2$ is normal in P_2. This shows that $P_2 = Q_2 \times K$ is abelian. It is elementary abelian by Lemma 4.1 and the fact that both K and $Q_2 = P_{2\,\beta} \simeq T^{(1)}$ are elementary abelian. By definition, P is normal in G^+ and, if $g \in G \setminus G^+$, then $P_1^g = P_2$ and $P_2^g = P_1$, so P is normal in G. By parts (1) and (2), $|P| = |Q_1| \cdot |K| \cdot |Q_2| = p^{a+b+a} = |E|$, and $P_{\alpha\beta} = 1$, so P acts regularly on E. Finally, $K \leqslant Z(P)$, since P_1 and P_2 are abelian. □

Cronheim [8, p. 3] calls a group P together with subgroups Q_1 and Q_2 satisfying the conditions of Lemma 4.3 a *T-group*. Recall that a *coset geometry* $K(P, Q_1, Q_2)$ is an incidence structure admitting P as a flag-transitive group [10, 1.2.17]. This incidence structure has points labelled by the right Q_1-cosets in P and the lines labelled by the right Q_2-cosets in P. A point is incident with a line iff the cosets labelling them intersect non-trivially.

It follows from Lemma 4.3.3 and [10, 1.2.17] that the incidence structure $(\Delta^{(1)}, \Delta^{(2)}, E)$ is isomorphic with the coset geometry $K(P, Q_1, Q_2)$. We give such an isomorphism f explicitly. Take $\alpha' \in \Delta^{(1)}$ and $\beta' \in \Delta^{(2)}$. By Lemma 4.3.2, there exist unique $q_1 \in Q_1$, $q_2 \in Q_2$ and $k_1, k_2 \in K$ such that $\alpha' = \alpha^{q_2k_2}$ and $\beta' = \beta^{q_1k_1}$. Define $f(\alpha') = Q_1q_2k_2$ and $f(\beta') = Q_2q_1k_1$ to be Q_i-cosets in P. By Lemma 4.3.3, $(\alpha', \beta') \in E$ iff there is $x \in P$ such that $\alpha' = \alpha^x$ and $\beta' = \beta^x$. This in turn occurs iff $x \in Q_1x \cap Q_2x = Q_1q_2k_2 \cap Q_2q_1k_1$. Therefore f is an incidence structure isomorphism.

Thus the incidence structure $(\Delta^{(1)}, \Delta^{(2)}, E)$, and hence our graph Γ, can be reconstructed from the group P and its two subgroups Q_i via $K(P, Q_1, Q_2)$. Recall that for any x and y in a group, the *commutator* of x with y is defined to be $[x, y] = x^{-1}y^{-1}xy$.

LEMMA 4.4 (Cronheim [8, Proposition 3]). *Take $\alpha' \in \Delta^{(1)}$ and $\beta' \in \Delta^{(2)}$. Then, by Lemma 4.3.2, there exist unique $q_1 \in Q_1$, $q_2 \in Q_2$ and $k_1, k_2 \in K$ such that $\alpha' = \alpha^{q_2k_2}$ and $\beta' = \beta^{q_1k_1}$. Then:*
(1) *$(\alpha', \beta') \in E$ iff $[q_1k_1, q_2k_2] = [q_1, q_2] = k_1k_2^{-1}$.*
(2) *$C_{P_1}(q_2) = K \times C_{Q_1}(q_2)$ has order k, for each non-trivial $q_2 \in Q_2$, and symmetrically with subscripts 1 and 2 interchanged.*

(3) *The commutator map:* $\varphi\colon Q_1 \times Q_2 \to K$ *given by* $\varphi(x, y) = [x, y]$ *specializes to surjective maps* $[*, q_2]\colon Q_1 \to K$, *and* $[q_1, *]\colon Q_2 \to K$ *for each* $q_i \in Q_i \setminus \{1\}$.
(4) $K = Z(P)$.

Proof. By the coset geometry construction, there is $x \in Q_1(q_1k_2) \cap Q_2(q_1k_1)$ iff $(\alpha', \beta') \in E$. This is equivalent to the existence of $x_i \in Q_i$ for $i = 1, 2$ such that $x_1q_2k_2 = x_2q_1k_1$ $(=x)$. In this case,

$$\beta' = \beta^{q_1k_1} = \beta^{x_2q_1k_1} = \beta^{x} = \beta^{x_1q_2k_2} = \beta^{q_2(q_2^{-1}x_1q_2k_2)} = \beta^{q_2^{-1}x_1q_2k_2}.$$

But q_1k_1, $q_2^{-1}x_1q_2k_2 \in P_1 \trianglelefteq P$, and P_1 acts regularly on $\Delta^{(2)}$ by Lemma 4.3.2, so $q_1k_1 = q_2^{-1}x_1q_2k_2$; whence $x = q_2q_1k_1$. A similar argument with α instead of β leads to $q_1q_2k_2 = x = q_2q_1k_1$, and so $[q_1k_1, q_2k_2] = [q_1, q_2] = k_1k_2^{-1}$, since $K \leqslant Z(P)$. Conversely, if $[q_1, q_2] = k_1k_2^{-1}$, then $q_1q_2k_2 = q_2q_1k_1 \in Q_1(q_2k_2) \cap Q_2(q_1k_1)$ and the first claim follows.

For $q_2 \in Q_2 \setminus \{1\}$, $C_{P_1}(q_2) = K \times C_{Q_1}(q_2)$, since $K \leqslant Z(P)$. By Lemma 2.1.4, the number of $q_1k_1 \in P_1$ such that $(\alpha, \beta^{q_1k_1}) \in E$ and $(\alpha^{q_2}, \beta^{q_1k_1}) \in E$ is k/r. By part (1), $(\alpha, \beta^{q_1k_1}) \in E$ iff $1 = [1, q_1k_1] = k_1^{-1}$ and, also by part (1), $(\alpha^{q_2}, \beta^{q_1}) \in E$ iff $[q_2, q_1] = 1$. Thus $C_{Q_1}(q_2)$ has order k/r and parts (2) and (3) follow. Finally, suppose that $Z(P) > K$. Then, by Lemma 4.3.3, $Z(P)$ contains a non-trivial element of the form q_1q_2, where $q_i \in Q_i$. At least one of q_1 and q_2 must be non-trivial; say, $q_1 \neq 1$. Now each $x \in Q_2$ commutes with $q_1q_2 \in Z(P)$, and with q_2 since Q_2 is abelian, so x commutes with $(q_1q_2)q_2^{-1} = q_1$. This shows $1 \neq q_1 \in C_{Q_1}(Q_2)$, contrary to part (2). □

If the map φ of Lemma 4.4.3 is known, then the group P can be presented as the free product of the elementary abelian groups K, Q_1 and Q_2 modulo the relations: K and each Q_i commute elementwise, and $q_1^{-1}q_2^{-1}q_1q_2 = \varphi(q_1, q_2)$ for $q_i \in Q_i$. Thus φ uniquely determines the isomorphism type of the group P together with its two distinguished subgroups Q_1 and Q_2. The coset geometry $K(P, Q_1, Q_2) \simeq (\Delta^{(1)}, \Delta^{(2)}, E)$ and its incidence graph Γ are consequently uniquely determined by φ. This proves the first part of the following crucial corollary to Lemma 4.4.

Proposition 4.5. *Let* Γ *be the incidence graph of the coset geometry* $K(P, Q_1, Q_2)$, *where* Q_1, Q_2, K *and the map* φ *satisfy the conditions in Lemma* 4.4. *Then:*
(1) Γ *is a distance-transitive antipodal* p^b*-fold cover of* K_{p^a,p^a} *whenever* $\mathrm{Aut}\,P$ *contains a subgroup* A *such that* $(Q_1 \cup Q_2)\setminus\{1\}$ *and* $K \setminus \{1\}$ *are the orbits of* A *in its action on the elements of* P.
(2) *The isomorphism type of* Γ *is uniquely determined by* φ.
(3) *If the groups* $Q_1^\flat$, $Q_2^\flat$ *and* $K^\flat$ *with the map* $\varphi^\flat$ *also satisfy the conditions of Lemma* 4.4, *then the corresponding incidence graph* $\Gamma^\flat$ *is isomorphic to* Γ *iff there are group isomorphisms* $f_i\colon Q_i \to Q_i^\flat$ *and* $f\colon K \to K^\flat$ *such that*

$$\varphi^\flat(f_1(q_1), f_2(q_2)) = f(\varphi(q_1, q_2)) \qquad \textit{for all } q_i \in Q_i.$$

Proof. Suppose that Γ is the incidence graph of the coset geometry $K(P, Q_1, Q_2)$. Then P is edge-transitive on Γ by Lemma 4.3.3, but has two orbits on the vertices of Γ. Take $a \in A$ and $x \in Q_1 \setminus \{1\}$ so that $x^a \in Q_2$. Since $(Q_1 \cup Q_2)\setminus\{1\}$ is an orbit of A, it follows that $Q_i^a = Q_{i-3}$ for $i = 1, 2$ and $\langle P, a\rangle$ is vertex-transitive on Γ. Let $A^+ = N_A(Q_1)$.

Let α denote the vertex Q_1 of Γ. For each i, consider $\Gamma_i(\alpha)$ as the union of the right cosets (of Q_1, if i is even, or of Q_2 if i is odd) contained in this set. Then $\Gamma_i(\alpha)$ is invariant under the right multiplication by $Q_1\colon \Gamma_0(\alpha) = Q_1$, $\Gamma_1(\alpha) = Q_2Q_1$, $\Gamma_2(\alpha) =$

$Q_1Q_2Q_1 \setminus Q_1$. Moreover, it follows from Lemmas 4.4.3 and 4.3.3 that $\Gamma_1(\alpha) \cup \Gamma_3(\alpha) = Q_2Q_1Q_2Q_1 \supseteq Q_2[Q_2, Q_1]Q_1 = Q_2P$ and $\Gamma_0(\alpha) \cup \Gamma_2(\alpha) \cup \Gamma_4(\alpha) = Q_1Q_2Q_1Q_2Q_1 \supseteq Q_1[Q_1, Q_2]Q_2 = Q_1P$. Hence Γ has diameter 4. The transitivity of A^+ on the non-trivial elements of Q_i, for $i = 1, 2$, implies the transitivity of $\langle A^+, Q_1\rangle$ on $\Gamma_{4-i}(\alpha)$ and the transitivity of A^+ on the non-trivial elements of K implies the transitivity of A^+ on $\Gamma_4(\alpha)$. This shows that $\langle A, P\rangle$ acts distance—transitively on Γ. The fact that Γ is a p^b-fold antipodal cover of K_{p^a,p^a} follows on examining the parameters of Γ.

Now consider another incidence graph $\Gamma^\flat$ of a coset geometry $K(P^\flat, Q_1^\flat, Q_2^\flat)$, where $P^\flat$, $Q_1^\flat$ and $Q_2^\flat$, together with the subgroup $K^\flat$ and map $\phi^\flat$, also satisfy the conditions of Lemma 4.4. Suppose first that there are maps f_i and f satisfying the conditions in the statement. Since each element of P (respectively $P^\flat$) has a unique expression as q_1q_2k (respectively $q_1^\flat q_2^\flat k^\flat$) with $q_i \in Q_i$, $k \in K$ ($q_i^\flat \in Q_i^\flat$, $k^\flat \in K^\flat$), the map $g(q_1, q_2, k) := f_1(q_1)f_2(q_2)f(k)$ is well defined and it is straightforward to check that g is a group isomorphism $P \to P^\flat$. Then g induces an isomorphism of the coset geometries $K(P, Q_1, Q_2) \to K(P^\flat, Q_1^\flat, Q_2^\flat)$, and hence it also induces a graph isomorphism $\Gamma \to \Gamma^\flat$.

Conversely, suppose that $\psi: \Gamma \to \Gamma^\flat$ is a graph isomorphism. By our classification completed so far we know that both $Aut\,\Gamma$ and $Aut\,\Gamma^\flat$ are of affine type with normal subgroups P and $P^\flat$, respectively. Thus ψ induces a group isomorphism $g: Aut\,\Gamma \to Aut\,\Gamma^\flat$ which maps P onto $P^\flat$. Moreover, since $Aut\,\Gamma$ is transitive on arcs, we may choose g to map the cosets Q_1 and Q_2 to $Q_1^\flat$ and $Q_2^\flat$, respectively. Thus f_i defined as the restriction of g to Q_i is a group isomorphism $f_i: Q_i \to Q_i^\flat$ for $i = 1, 2$ and also f defined as the restriction of g to K is an isomorphism $K \to K^\flat$ (since $[Q_1, Q_2] = K$ and $[Q_1^\flat, Q_2^\flat] = K^\flat$). Moreover, for all $q_1 \in Q_1$ and $q_2 \in Q_2$ we have that $\varphi^\flat(f_1(q_1), f_2(q_2)) = [g(q_1, g(q_2)]$ (by the definition of $\varphi^\flat$, f_1 and f_2), which is equal to $g([q_1, q_2]) = g(\varphi(q_1, q_2))$ (by the definition of φ and since g is a group homomorphism). $\square$

Switching to additive notation, we regard Q_i as an a-dimensional vector space over $GF(p)$, and K as a b-dimensional space over $GF(p)$. Then the map φ is a $GF(p)$-bilinear map. Just as in [20, Corollary 2.3] it follows that φ induces a linear map $\varphi^*: Q_1 \otimes Q_2 \to K$ from the tensor product (over the integers) of Q_1 and Q_2 into K; and φ^* uniquely determines φ and vice versa. Lemma 4.4.3 implies that the contraction of φ relative to any non-trivial element of Q_i is surjective. Indeed, this is the reason for *non-singular* in the title of [20].

We say that an arbitrary $GF(p)$-bilinear map $\varphi: Q_1 \times Q_2 \to K$ is *totally surjective* if all the maps $\varphi(\bigstar, q_2)$ and $\varphi(q_1, \bigstar)$, $q_i \neq 0$, $i = 1, 2$ (as in Lemma 4.4.3) are surjective and extend this name to the associated $\varphi^*: Q_1 \otimes Q_2 \to K$.

As in [20, Theorem 3.1], we can say more. Since P_1, P_2 and K are all invariant under $G^+ = PG_{\alpha\beta}$, and since P acts trivially by conjugation on $P_1/K \simeq Q_1$, $P_2/K \simeq Q_2$ and K, $Q_1 \otimes Q_2$ and K can both be regarded as modules over the group ring $\mathcal{R} = GF(p)G_{\alpha\beta}$. When this is done, φ^* becomes a totally surjective $\mathcal{R}$-module homomorphism.

Note that our modules arise as additive versions of conjugation within G, which we write as: g maps x to x^g $(= g^{-1}xg)$. Thus, we write the additive version as a right module over $\mathcal{R}$.

Let M be the kernel of φ^*. Then M is an $\mathcal{R}$-submodule of $Q_1 \otimes Q_2$, and since $G_{\alpha\beta}$ is transitive on $K \setminus \{1\}$, K is an irreducible $\mathcal{R}$-module and hence M is a maximal submodule. Thus we may identify K with the quotient module $(Q_1 \otimes Q_2)/M$ and φ^* with the associated canonical quotient map $q_1 \otimes q_2 \mapsto (q_1 \otimes q_2) + M$ and hence φ with the map $(q_1, q_2) \mapsto (q_1 \otimes q_2) + M$. Moreover, $G_{\alpha\beta}$ acts transitively on the non-trivial

M-cosets. By [8, Proposition 8], as in [20, Theorem 2.1], classifying the possible commutator maps φ amounts to classifying all maximal $\mathcal{R}$-submodules M of $Q_1 \otimes Q_2$ of codimension b such that:

(1) $G_{\alpha\beta}$ acts transitively on the non-trivial M-cosets;

(2) the canonical epimorphism $\varphi^*: Q_1 \otimes Q_2 \to K = Q_1 \otimes Q_2/M$ is a totally surjective $\mathcal{R}$-module homomorphism.

If b divides a and if Q_1, Q_2 and K can be regarded as $GF(p^b)$-vector spaces in such a way that φ satisfies the above conditions and is $GF(p^b)$-bilinear then, as the next lemma shows, the *generic case* occurs.

Lemma 4.6. *Suppose that b divides a, that Q_1, Q_2 and K are all $GF(p^b)$-vector spaces and that φ is $GF(p^b)$-bilinear. Then case (1) of the Main Theorem holds. These conditions are met in particular if $b = 1$ or if $\mathrm{Aut}\, P$ contains a pair of cyclic subgroups R_1 and R_2 of order prime to p with $[R_1, R_2] = 1$ such that R_i acts trivially on $\Sigma^{(i)}$ and irreducibly on K for $i = 1$ and 2.*

Proof. We continue to use additive notation in the elementary abelian groups K, Q_1 and Q_2 in order to employ the language of bilinear forms. Pick $\{x_1, \ldots, x_{a/b}\} \subseteq Q_1$ to be a $GF(p^b)$-basis of Q_1 and let $y_i^* = [x_i, *]: Q_2 \to K$ be the associated $GF(p^b)$-linear functional appearing in Lemma 4.4.3. If the y_i^* were dependent (in the dual space of Q_2), then there would be a non-trivial element in $\bigcap_{i \geq 1} C_{Q_2}(x_i) = C_{Q_2}(Q_1) \leq Z(P)$, contrary to Lemma 4.4.4. Thus, $\{y_1^*, \ldots, y_{a/b}^*\}$ is a basis of the dual space of Q_2 and its dual basis $\{y_1, \ldots, y_{a/b}\} \subseteq Q_2$ has the property that, for each i, j, the commutator $[x_i, y_j] = \delta_{i,j}$, where $\delta_{i,j}$ denotes the Kronecker delta function.

Now the matrix of the bilinear form φ of Lemma 4.4.3 relative to the bases $\{x_i\}$ and $\{y_i\}$ is the identity and this form is equivalent to the form arising in $PG_{(a/b)-1}(p^b)^{op}$. By Proposition 4.5, the graph Γ is therefore isomorphic to $PG_{(a/b)-1}(p^b)^{op}$.

Of course, any bi-additive form is bilinear over the prime field, so the conditions hold if $b = 1$. It remains to deal with groups R_i as specified. Geometrically, R_2 fixes the point α and acts trivially on the parallel classes $\Sigma^{(2)}$, so it normalizes $Q_1 = P_{1\,\alpha}$. By Lemma 4.3.2, Q_1 acts regularly on the parallel classes $\Sigma^{(2)}$. It follows that R_2 must act trivially on Q_1. Therefore R_2 and Q_1 commute elementwise.

Now view Q_1, Q_2 and K as $\mathcal{R}$-modules, where $\mathcal{R} = GF(p)R_2$. We have just shown that Q_1 is a trivial $\mathcal{R}$-module, We claim that Q_2 and K, and hence $P_2 = K \times Q_2$, are homocyclic $\mathcal{R}$-modules. (This means that the minimal polynomial of the action of a generator of R_2 on P_2 is irreducible.) To show this, we establish that any irreducible $\mathcal{R}$-submodule of Q_2 is isomorphic to (any irreducible submodule of) K.

We claim that $C_{Q_2}(R_2) = 1$. Suppose, to the contrary, that $q_2 \in Q_2 \setminus \{1\}$ is centralized by R_2. By Lemma 4.4.3, the map $q_1 \mapsto [q_1, q_2]$ has image K. Since R_2 centralizes Q_1 and q_2, it follows that R_2 centralizes K, which is a contradiction. Let M be a minimal $\mathcal{R}$-submodule of Q_2 which is non-trivial by the previous sentence, and let $q_1 \in Q_1 \setminus \{1\}$. We claim that $\mathcal{M} = \langle M, M^{q_1} \rangle$ is homocyclic. If q_1 centralizes M, then $\mathcal{M} = M$, and the claim is trivial. Suppose that there exists $m \in M \setminus C_M(q_1)$. Then $\mathcal{M}$ is an $\mathcal{R}$-submodule of P_2 containing $\mathcal{R}$-submodules M, M^{q_1} and $0 \neq \langle [m, q_1]^{R_2} \rangle \leq K$. These three $\mathcal{R}$-submodules have pairwise trivial intersections, by the minimality of M and by Lemma 4.3.2. Since any two generate $\mathcal{M}$, $\mathcal{M}$ is a homocyclic $\mathcal{R}$-module.

Since $q_1 \in Q_1$ was arbitrary, Lemma 4.4.3 implies that KM is a homocyclic $\mathcal{R}$-module. But R_2 has order relatively prime to the characteristic p, so it acts completely reducibly on P_1 and the arbitrary choice of M in the above argument implies that any irreducible $\mathcal{R}$-submodule of Q_2 is isomorphic to any of those appearing within K. Thus P_2 itself is homocyclic as an $\mathcal{R}$-module.

Now R_2 acts faithfully and irreducibly on K, so $End_{\mathscr{R}}(K)$ is the field $GF(p^b)$ by Schur's lemma. Let f be a polynomial in $GF(p)[x]$ evaluated at $r_2 \in R_2$ and viewed as a $GF(p)$-linear function on P_2. Define f to act trivially on Q_1. Since φ is bi-additive and R_2 centralizes Q_1, it follows that φ commutes with f. The paragraph preceding Proposition 4.5 implies that $f \in Aut\, P$ and, without loss of generality, we may suppose that $|R_2| = p^b - 1$.

Thus K is a 1-dimensional $GF(p^b)$-vector space, and there is a $GF(p^b)$-valued character λ_2 of $R_2 \simeq GF(p^b)^*$ such that the image of k under r (under conjugation) is $k^r = k\lambda_2(r)$ for all $k \in K$, $r \in R_2$. Since P_2 is a homocyclic $\mathfrak{R}$-module, in fact $x^r = x\lambda_2(r)$ for any $x \in P_2$ as well.

In a similar way, R_1 may be used to endow P_1 with a $GF(p^b)$-vector space structure, and this allows us to assume without loss that $|R_1| = p^b - 1$. Also, there is an $GF(p^b)$-valued character λ_1 of R_1 such that $x^r = x\lambda_1(r)$ for any $x \in P_1$, $r \in R_1$. Moreover, the assumption that R_1 and R_2 commute implies that $GF(p^b) = End_{\mathscr{R}_1}(K) = End_{\mathscr{R}_2}(K)$, where $\mathscr{R}_i = GF(p)R_i$ for $i = 1, 2$.

It remains to check that φ is $GF(p^b)$-bilinear. Let $0 \neq \lambda = \lambda_1(r_1) = \lambda_2(r_2)$ for $r_1 \in R_1$ and $r_2 \in R_2$. For $x \in Q_1$ and $y \in Q_2$, $y^{r_1} = y$ and $x^{r_2} = x$. Moreover, we have $\varphi(\lambda x, y) = \varphi(x^{r_1}, y) = \varphi(x^{r_1}, y^{r_1}) = [x^{r_1}, y^{r_1}] = [x, y]^{r_1} = (\varphi(x, y))\lambda_1(r_1) = \lambda\varphi(x, y)$. Using r_2 in place of r_1, we similarly obtain that $\varphi(x, \lambda y) = \lambda\varphi(x, y)$. □

Note that Proposition 4.5 allows us to recover any graph in the affine case from the bi-additive commutator form φ or, equivalently, from the linear form φ^*. Lemma 4.6 makes this recovery explicit for the incidence graphs $\Gamma = PG_n(q)^{op}$ of Construction 1.1. A group P supporting this coset geometry and realizing the above form as the commutator map is $P = O_p(Aut\, \Gamma)$, and has elements of the form

$$\begin{pmatrix} 1 & x & z \\ 0 & I_{n-1} & y \\ 0 & 0 & 1 \end{pmatrix}, \qquad \text{where } x \in Mat_{1,n-1}(GF(q)),\ y \in Mat_{n-1,1}(GF(q)),\ z \in GF(q).$$

The arguments of this section are extensions from the case $a = b$ be given in [20], where projective planes in Lenz class V are studied by these methods. Because there are no such planes of order p^2, p prime [10, 5.3.6], we have the following:

COROLLARY 4.7. *If $a = b \leqslant 2$, then case* (1) *of the Main Theorem holds.*

5. THE TENSOR MODULE UNDER A SINGER CYCLE

If G is the full automorphism group of the incidence graph of $PG_{a-1}(p)^{op}$, then $H_0 = \Gamma L(a, p)$. It follows that every finite transitive linear group can occur in, say Lemma 2.2.1, as a homomorphic image of the group H_0 for a graph of the type we are studying. In order to avoid a proliferation of cases, we adopt the strategy of working from a carefully chosen type of subgroup that exists for all finite transitive linear groups and implementing the commutator form classification scheme outlined just before Lemma 4.6 relative to these groups. The subgroups that we use are Singer cycles.

A group $S \leqslant GL(a, p)$ is a *Singer group* if it acts regularly on the non-zero elements of the underlying vector space $V = GF(p)^a$. We call a cyclic irreducible linear group $T \leqslant GL(a, p)$ a *Singer cycle.* Note that the centralizer of T in $GL(a, p)$ is a cyclic Singer group, by Schur's lemma. Note that the groups R_i appearing in Lemma 4.6 act as Singer cycles on K.

Recall that for any integers $n \geqslant 2$ and $m \geqslant 2$, a prime divisor s of $n^m - 1$ is called a *primitive prime divisor* of $n^m - 1$ if s does not divide $n^i - 1$ for any $i < m$. In 1892, Zsigmondy [25] showed that if $m \geqslant 3$ and $(n, m) \neq (2, 6)$, then $n^m - 1$ always has a primitive prime divisor. Such divisors may or may not exist if $m = 2$. In fact, $n^2 - 1$ has a primitive prime divisor unless $n = 2^e - 1$ for some e; and if, further, $n = p^c$ for p a prime and $n^2 - 1$ has no primitive prime divisor, then $n = p = 2^e - 1$ is a Mersenne prime.

Clearly, if s is a primitive prime divisor of $p^a - 1$, then any Sylow s-subgroup of $GL(a, p)$ is a Singer cycle—and the Sylow s-subgroup is obviously non-trivial in every doubly transitive group of degree p^a. We show that actually, in all cases, $G_{\alpha\beta}$ must contain a subgroup T that acts as a Singer cycle on both Q_1 and Q_2. We now study the decomposition of the $GF(p)T$-module $Q_1 \otimes Q_2$.

In order to simplify notation and make clear both the structure of this argument and the structure of the proof of the Main Theorem, we present this decomposition separately. In a formal sense this decomposition is a character-theoretic triviality, but it is necessary for us to do it explicitly in order to identify the Constructions 5.6 and 5.7.

Suppose that T_i is a Singer cycle acting (on the right) on the $GF(p)$-vector space V_i of dimension a, for $i = 1, 2$. Let N_i (S_i) be the normalizer (centralizer) of T_i in $GL(V_i)$, for $i = 1, 2$. By Schur's lemma, $S_i \geqslant T_i$ is the multiplicative group of a finite division ring E_i and hence $E_i \simeq GF(p^a)$, and $N_i \simeq \Gamma L(1, p^a)$ is the semidirect product of S_i by $A_i = Aut\, E_i$ for $i = 1, 2$.

Observe that V_i is a 1-dimensional (right) E_i-vector space, for $i = 1, 2$. Fix non-zero $v_i \in V_i$ and use these to define E_i as right N_i-modules:

$$(v_i)(e_i n_i) := ((v_i)e_i)n_i \qquad \text{for } e_i \in E_i,\ n_i \in N_i; \quad i = 1, 2.$$

Here we are defining the right N_i-module structure of E_i. For arbitrary elements $e_i \in E_i$ and $n_i \in N_i$, $e_i N_i \in E_i$ is defined by the above equality.

Let $Hom_+(E_1, E_2)$ be the additive group of additive homomorphisms from the additive group of E_1 to the additive group of E_2. Then $Hom_+(E_1, E_2)$ is a right $(N_1 \times N_2)$-module in the usual way:

$$(f(n_1, n_2))(e_1) := (f(e_1 n_1^{-1}))n_2 \qquad \text{for } f \in Hom_+(E_1, E_2),\ n_i \in N_i;\ i = 1, 2,\ e_1 \in E_1.$$

Here we are defining the right $(N_1 \times N_2)$-module structure of $Hom_+(E_1, E_2)$. For an arbitrary $f \in Hom_+(E_1, E_2)$, $f(n_1, n_2) \in Hom_+(E_1, E_2)$ is defined by the above equality. Note that the restriction of this module of $1 \times S_2 \leqslant N_1 \times N_2$ can also be described as endowing $Hom_+(E_1, E_2)$ with a (right) E_2-vector space structure:

$$(f e_2)(v_2) = (f(v_2))e_2; \qquad \text{for } f \in Hom_+(E_1, E_2) \quad \text{and} \quad e_2 \in E_2.$$

LEMMA 5.1. *Fix an arbitrary field isomorphism $\phi: E_1 \to E_2$. Let σ_1 be a generator of S_1 and let $\sigma_2 = \phi(\sigma_1) \in S_2$. Denote the E_2-subspace generated by $\phi \in Hom_+(E_1, E_2)$ by $\mathscr{E}$. Finally, denote the group of field automorphisms of E_2 by $Aut\, E_2$ and define $\kappa \in Aut\, E_2$ by $\kappa(\sigma_2) = (\sigma_2)^{p^k}$. Then:*

(1) *$\kappa\mathscr{E}$ is $S_1 \times S_2$-invariant and, for x and y integers,*

$$\kappa\phi(\sigma_1^x, \sigma_2^y) = \kappa\phi(1, \sigma_2^{x - yp^k}).$$

(2) *We have the $S_1 \times S_2$-module decomposition: $Hom_+(E_1, E_2) = \bigoplus_{\lambda \in Aut\, E_2} \lambda\mathscr{E}$.*

PROOF. In view of the E_2-vector space structure of $Hom_+(E_1, E_2)$, it suffices to verify the formula in part (1) when $y = 0$. Fix $e_1 \in E_1$. Then

$$(\kappa\phi(\sigma_1^x, 1))(e_1) = \kappa(\phi(e_1\sigma_1^{-x})) = \kappa(\phi(e_1))\kappa(\phi(\sigma_1)^{-x}),$$

since both ϕ and κ are field isomorphisms. Thus, in turn the latter expressions, equal the following:

$$\kappa\phi(e_1)\kappa(\sigma_2)^{-x} = (\kappa\phi(1, \sigma_2^{-xp^k}))(e_1),$$

by the definition of σ_2, the definition of κ and the action of $N_1 \times N_2$ on $Hom_+(E_1, E_2)$. Since $e_1 \in E_1$ was arbitrary, this proves part (1).

Now $\sigma_2^{p^k} = \sigma_2^{p^{k'}}$ only if $k = k'$, so part (1) exhibits $|Aut\, E_2|$ non-isomorphic $S_1 \times 1$-submodules of $Hom_+(E_1, E_2)$, each of which is of E_2-dimension 1. Since $|Hom_+(E_1, E_2)| = p^{a^2} = |E_2|^a$, the E_2-dimension of $Hom_+(E_1, E_2)$ is a and part (2) follows from part (1). □

Return to the notation at the end of Section 4. For $i = 1, 2$, regard Q_i as a $GF(p)$-vector space of dimension a. Recall [9, 43.7, 43.14] the dual space of Q_1 is $Q_1^* = Hom_+(Q_1, GF(p))$ and is an N_1-module just as above $((q_1^* n_1)(x) = q_1^*(xn_1^{-1})$, for $q_1^* \in Q_1^*$, $x \in Q_1$ and $n_1 \in N_1)$. The N_1-module Q_1^* is called *contragredient* to the N_1-module afforded by Q_1. There is a natural isomorphism of $(N_1 \times N_2)$-modules:

$$\lambda\colon Hom(Q_1^*, Q_2) \simeq Q_1 \otimes Q_2 \qquad \text{where } \lambda(f) = q_1 \otimes q_2 \quad \text{when } f(q_1^*) = q_1^*(q_1)q_2.$$

(Warning: This only specifies λ as a map between the rank 1-linear functions and the decomposable tensors. An arbitrary element of $Hom(Q_1^*, Q_2)$ can be expressed as a sum of rank 1-functions and so the full definition of λ requires extension of this equation by linearity.)

We apply Lemma 5.1 with $V_1 = Q_1^*$ and $V_2 = Q_2$ to obtain the desired decomposition. The N_i-module structure of E_i, for $i = 1, 2$, implies that there is an $(N_1 \times N_2)$-module isomorphism

$$\mu\colon Hom_+(E_1, E_2) \simeq Hom(V_1, V_2) = Hom(Q_1^*, Q_2).$$

Corollary 5.2 (cf. [20, Example 3.2]). *Continue the meanings of $N_i, S_i, \sigma_i, \phi, E_i, \mathscr{E}, \kappa, k, \lambda$ and μ introduced in this section. Then:*

(1) *We have $Q_1 \otimes Q_2 = \bigoplus_{\kappa \in Aut\, E_2} \lambda\mu(\kappa\mathscr{E})$ as $(S_1 \times S_2)$-modules.*

(2) *For $\tau = (\sigma_1^x, \sigma_2^y) \in S_1 \times S_2$, $\epsilon \in \mathscr{E}$, $\lambda\mu(\kappa\epsilon)(\tau) = \lambda\mu(\kappa\epsilon)(1, \sigma_2^{x+yp^k})$.*

(3) *Suppose that $\alpha_i \in Aut\, E_i$. Then, for $\epsilon \in \mathscr{E}$, $\lambda\mu(\kappa\epsilon)(\alpha_1, \alpha_2) = \lambda\mu(\alpha_2\kappa\epsilon\alpha_1)$.*

Proof. Set $V_1 = Q_1^*$ and $V_2 = Q_2$. Then the first two parts are obtained from parts (1) and (2) of Lemma 5.1 by means of the $(N_1 \times N_2)$-module isomorphisms $\lambda\mu$: $\mathrm{Hom}_+(E_1, E_2) \simeq Q_1 \otimes Q_2$. The third part follows from this isomorphism, the definition of the $(N_1 \times N_2)$-module structure of $Hom(Q_1^*, Q_2)$ and the fact that Q_1^* is an N_1-module contragredient to the N_1-module afforded by Q_1. □

Since $K \cap G_{\alpha\beta} = 1$, $G_{\alpha\beta}$ acts faithfully on $\Sigma_1 \times \Sigma_2$ and so we may regard $G_{\alpha\beta}$ as a subgroup of $Aut\, Q_1 \times Aut\, Q_2$. As pointed out in Section 4, the commutator form on P gives rise to a totally surjective $G_{\alpha\beta}$-homomorphism of $\varphi^*\colon Q_1 \times Q_2 \to K$. Corollary 5.2 leads directly to the following:

Corollary 5.3. *Suppose that $T \leqslant G_{\alpha\beta}$ maps to a subgroup of $S_1 \times S_2$ that acts as a Singer cycle on each Q_i, $i = 1, 2$. Fix $x_i \in Q_i$ and identify $e_i \in E_i$ with $q_i = e_i x_i \in Q_i$, $i = 1, 2$.*

Suppose that ker φ^* contains all but one of the summands in the decompostion given in Corollary 5.2.1. *Then, after appropriate normalization, the bi-additive map φ may be written*

$$\varphi(e_1x_1, e_2x_2) = \nu(\phi(e_1)e_2), \qquad \textit{for some abelian group homomorphism } \nu\colon E_2 \to K.$$

This occurs whenever T acts trivially on K, in which case T is cyclic and Q_1 and Q_2 are contragredient T-modules.

Proof. Since some summand in Corollary 5.2.1 is not in the kernel of φ^*, we may change ϕ in Lemma 5.1 if necessary and suppose that $\mathscr{E} \nleqslant \mathit{ker}\, \varphi^*\lambda\mu$. If $\mathscr{E}$ is the only summand in Corollary 5.2.1 not in the kernel of $\varphi^*\lambda\mu$, then φ^* factors through the natural projection map $\pi\colon Q_1 \otimes Q_2 \to \lambda\mu\mathscr{E}$ arising from the decomposition appearing in Corollary 5.2.1. Since π is $(S_1 \times S_2)$-invariant, Corollary 5.2.2 implies that $\pi(q_1 \otimes q_2) = \lambda\mu(\phi(q_1)q_2)$. The first claim follows.

Suppose that T acts trivially on K. Then $\nu\lambda\mu\mathscr{E}$ is a non-trivial homomorphic image of $\mathscr{E}$ affording a trivial T-module. If $(\sigma_1^x, \sigma_2^y) \in T$, then $\sigma_2^{x+y} = 1$, and so $y \equiv -x \pmod{p^a - 1}$, by Corollary 5.2.2. If a second summand of Corollary 5.2.1, say $\kappa\mathscr{E}$, where $\kappa(x) = x^{p^k}$, $k < a$, is not contained in $\mathit{ker}\, \varphi^*\lambda\mu$ as well, then $y \equiv p^k x\ (\mathit{mod}\, p^a - 1)$ also. Thus $0 \equiv (p^k - 1)x\ (\mathit{mod}\, p^a - 1)$, contrary to the hypothesis that T acts as a Singer cycle on Q_1 and the fact that each subgroup of a cyclic group is uniquely determined by its order.

Finally, the non-trivial elements of $\mathscr{E} = \phi E_2 \leqslant \mathit{Hom}(Q_1^*, Q_2)$ are T-isomorphisms of Q_1^* with Q_2, are contragredient T-modules. Corollary 5.2.2 and the trivial action of T on $\mathscr{E}$ imply that T acts faithfully on Q_1, so T is cyclic. □

The situation described in Lemma 4.6 arises in the generic case with ν equal to the trace map from one field to another. We conclude this section by showing that the hypothesis of Lemma 4.6 cannot go too far wrong if T is sufficiently large and with the two cases of the Main Theorem turning up as cases in which this hypothesis fails. The reader not immediately concerned with these subtleties is encouraged to skip to the next section.

Suppose that $T \leqslant G_{\alpha\beta}$ maps to a subgroup of $S_1 \times S_2$ that acts as a Singer cycle on each Q_i, $i = 1, 2$. Let $\sigma \in \mathit{Aut}\, E_2$ be the Frobenius automorphism $\sigma(x) = x^p$, and let X_i be the summand of Corollary 5.2 associated with σ^i, $i = 1, \ldots, a$. When the hypothesis of Lemma 4.6 fails, the set $J = \{j \mid X_j \subsetneq \mathit{ker}\, \varphi^*\}$ has at least two elements j and k, and

$$X_j/(X_j \cap \mathit{ker}\, \varphi^*) \simeq K \simeq X_k/(X_k \cap \mathit{ker}\, \varphi^*)$$

as T-modules. This condition is easy to check, because elements of E_2^* have the same minimal polynomial iff they are algebraically conjugate, so in the notation of Corollary 5.2.2 this condition is equivalent to

$$j, k \in J \text{ iff } x + yp^j \equiv p^i(x + yp^k) \pmod{|\tau|}, \qquad \text{for some integer } i.$$

When this occurs, we say that $x + yp^j$ and $x + yp^k$ are in the same *p-cyclotomic coset* $(\mathit{mod}\, |\tau|)$.

Lemma 5.4. *Assume that $p^a \neq 2^4$ and $t = (p^a - 1)/d$, where d is the greatest common divisor of $p^s - 1$ and a. Suppose that $T = \langle\tau\rangle$ has order t and acts faithfully on Q_1 and on Q_2. Then no three X_i are isomorphic T-modules.*

Proof. We may choose $\sigma_1 \in E_1$ in Lemma 5.1, so that $x = d$ in Corollary 5.2.2.

Then $y = y'd$ for some integer y' relatively prime to t. If three X_i afford isomorphic T-modules, then Corollary 5.2.2 implies that

$$p^i(dp^{k'} + y) \equiv dp^k + y \equiv p^j(dp^{k''} + y) \qquad (mod\, p^a - 1), \tag{1}$$

for distinct k, k' and k'' $(mod\, a)$ and some values of $i \not\equiv 0 \not\equiv j$ $(mod\, a)$, and $\{k, k', k''\} \subseteq J$. Collect the terms involving y in the left and the right congruence. Replace these with congruences modulo t and multiply the resulting congruences to obtain

$$y'(p^{i+k'} - p^k)(p^j - 1) \equiv y'(p^{j+k''} - p^k)(p^i - 1) \qquad (mod\, t).$$

Since y' is relatively prime to t, simplification leads to

$$p^{i+k} + p^{i+j+k'} + p^{j+k''} \equiv p^{i+k'} + p^{i+j+k''} + p^{j+k} \qquad (mod\, t), \tag{2}$$

to which the numerical Lemma 5.5 below applies.

Suppose that, in some order, the exponents on the left of (2) are congruent to the exponents on the right (modulo a). The assumption that k, k' and k'' be distinct implies that no corresponding terms are paired. Since $j + k'' \equiv i + j + k''$ $(mod\, a)$ contradicts $i \not\equiv 0$ $(mod\, a)$, it follows that $i + k \equiv i + j + k''$ $(mod\, a)$ and so $dp^k + yp^j \equiv dp^{j+k''} + yp^j = p^j(dp^{k''} + y)$ $(mod\, p^a - 1)$. Now the second part of (1) implies $y \equiv yp^j (mod\, p^a - 1)$, and so $t \mid (p^j - 1)$, since y' is relatively prime to t. But, by definition of t, either a primitive prime divisor of $p^a - 1$ divides t or $t = 21$ and $p^a = 2^6$ and so $a \mid j$.

In case $p^a = 3^4$, one can normalize so that $(k'', k, k') \equiv (-1, 0, 1)$ $(mod\, 4)$ and then observe that congruence 1 has no solutions. □

LEMMA 5.5. *Set* $t = (p^a - 1)/gcd(p^a - 1, a)$ *and suppose that* $a_1 + a_2 + a_3 = b_1 + b_2 + b_3$ *and*

$$p^{a_1} + p^{a_2} + p^{a_3} \equiv p^{b_1} + p^{b_2} + p^{b_3} \qquad (mod\, t).$$

Then there is a matching of the a_i *and the* b_i, *so corresponding pairs are congruent modulo a unless* $p^a \in \{2^4, 3^4\}$.

PROOF. If equality instead of congruence (modulo t) holds, then the minimum power of p appears at least twice. Subtract two such terms and repeat. If this does not result in a matching of the a_i and the b_i, then we started with something of the form: $p^{a_1} + p^{a_2} + p^{a_2} = p^{b_1} + p^{b_2} + p^{b_2}$, in which case either there is a matching or we have $2^{a_1} + 2^{b_1 - 1} + 2b^{b_1 - 1} = 2^{b_1} + 2^{a_1 - 1} + 2^{a_1 - 1}$ and $a_1 \neq b_1$ holds. This fails the sum of exponents condition.

Suppose that there is no matching and let k be the number of distinct (modulo a) values of exponents in the above congruence. Multiply the congruence by powers of p and reduce the exponents (modulo a) until the exponent 0 appears and the largest gap between the exponents (modulo a) precedes it. Now the maximum value of $\{a_i, b_i\} \leqslant a - \lceil a/k \rceil$ and equality holds unless at least one side, say the left-hand side of the congruence, is greater than t. When, for example $k = 6$, we have

$$(p^2 + p + 1)p^{a - \lceil a/6 \rceil - 2} \geqslant p^{a_1} + p^{a_2} + p^{a_2} > t = (p^a - 1)/d.$$

Since $d \mid a$, we can search for solutions to the resulting inequalities in two steps by considering the following:

$$\begin{array}{ccccll} (p^2 + p + 1)a & \geqslant & (p^2 + p + 1)d & > p^{2 + \lceil a/6 \rceil} & \text{when } k = 6, \\ (2p + 1)a & \geqslant & (2p + 1)d & > p^{1 + \lceil a/5 \rceil} & \text{when } k = 5, \\ 3a & \geqslant & 3d & > p^{\lceil a/4 \rceil} & \text{when } k = 4. \end{array}$$

If $a \geqslant 32$, the cruder inequality has no solution even for $p = 2$ and if $a > 6$, only $p \leqslant 5$ need be checked. In checking the remaining cases it helps to use Euler's Theorem $a \mid (p^{\phi(a)} - 1)$, which implies that $d \mid (p^{gcd(a,\, \phi(a))} - 1)$. The cases $p^a = 3^8, 2^{12}$ and 5^4 survive this arithmetic test but inspection shows that they lead to no solutions of the congruence. The congruence $1 + q + q^2 \equiv (1 + q + q^2)q\ (mod (q^6 - 1)/(q + 1))$ for $q = 2, 5$ or 8, survives all but the sum of exponents condition. □

Case 2 of the Main Theorem arises when $|J| \neq 1$, $p^a = p^b \neq 2^4$ and $T = \langle \tau \rangle$ is cyclic of order $(p^a - 1)/d$, where d divides both $p^a - 1$ and a. In this case we can identify E_2 with K via ν.

By Lemma 5.4, $|J| = 2$ and by replacing φ if necessary, assume that $J = \{0, 2j\}$ for some integer $1 \leqslant j < a$. Since for $x = p^j$ and $y = 1$, the equations $p^j(x + y) = p^{2j} + p^j = yp^{2j} + x$ imply that $x + y$ and $x + p^{2j}y$ are in the same p-cyclotomic coset $(mod\, p^a - 1)$, there are cyclic Singer groups T that act homocyclicly on $X_0 + X_{2j}$. As in the first paragraph of the proof of Corollary 5.3, the T-invariant forms for which $J = \{0, 2j\}$ may be obtained by means of the associated projection maps. Using $\pi_0 - c\kappa\pi_j$, $c \in E_2$, we obtain a T-invariant form φ:

$$\varphi(e_1x_1, e_2x_2) = \phi(e_1)e_2 - c(\phi(e_1)e_2^{p^{2j}})^{p^k}; \qquad c \in E_2 \setminus \{0\}.$$

If the form φ is used to define a multiplicative structure on the additive group of $GF(p^a)$ the resulting ring satisfies the distributive laws, but multiplication is not necessarily associative. Moreover, φ is totally surjective exactly when both cancellation laws hold. Such a ring satisfies all axioms for a field except for the distributive law, and is called a *semifield* or *non-associative division ring* or *distributive quasifield.* The original interest in finite semifields was probably inspired by the famous Wedderburn theorem that a finite ring satisfying all axioms for a field except commutative multiplication is, in fact, a field. In the 1950s A. A. Albert called semifields arising from φ of the above form *generalized twisted fields.* A clever choice of c is needed to ensure that φ is totally surjective.

CONSTRUCTION 5.6. *Albert observed that whenever $c = \sigma^k(x)x^{-1}\sigma^{2j+k}(y)y^{-1}$ has no solution in E_2, the above form has the property that $\varphi(x, y) = 0$ only if $x = 0$ or $y = 0$, which is exactly the condition of total surjectivity from Section* 4. *These algebraic structures are the generalized twisted fields* [10, *p.* 243]. *For historical reasons, the case $j + k = a$ bears the simpler name of twisted fields.*

Let N be the norm map from $GF(p^a)$ to the field fixed by α. The conditions of Proposition 4.5 *are met by the form φ arising from any twisted field for which $N(c)$ and $N(c^{-1})$ are distinct but algebraically conjugate* [6].

Case 6 of the Main Theorem also arises when $|J| = 2$, but when $p^a = 2^6 \neq p^b$. The group H_0 acts as a non-cyclic Singer group on both Q_1 and Q_2 and non-trivially on K. We show that this situation leads to the unique Example 5.7.

There are three types of Singer groups arising as subgroups of $GL(6, 2)$. Indeed, Sylow's theorem implies that such a group must have a (cyclic) normal subgroup of order 21 and hence arise as a subgroup of $\Gamma L(1, 64) = \langle \omega, \sigma \mid \omega^{63} = \sigma^6 = 1, \omega^\sigma = \omega^2 \rangle$. In addition to the Singer cycle $\langle \omega \rangle$ there are the Singer groups $H^\pm = \langle \omega^3, \omega^{\pm 1}\sigma^2 \rangle$. Each of the groups $H^\pm$ is isomorphic to the non-split central extension $H = \langle \tau, \pi \mid \tau^{21} = \pi^9 = 1, \tau^\pi = \tau^4 \rangle$ as an abstract group. The two linear groups $H^\pm \leqslant GL(6, 2)$ provide (the only) two inequivalent faithful irreducible $GF(2)$-representations $\rho^\pm$ of H $(\rho^\pm(\tau) = \omega^{\pm 3}, \rho^\pm(\pi) = \omega\sigma^2)$. The contragredient of ρ^+ is ρ^-. Since only even powers of σ appear in $\rho^\pm$, each is $GF(4)$-linear of dimension 3.

Suppose that Q_1 and Q_2 afford $\rho^{\pm}$ and ρ^{+} respectively. The representation $\rho^{\pm} \otimes \rho^{+}(\tau)$ decomposes into six summands X_i as in Corollary 5.2.1. The elements σ_1 and σ_2 can be chosen so that Corollary 5.2.2 reads $\lambda\mu(\kappa\phi)(\tau) = \lambda\mu(\kappa\phi)(1, \sigma_2^{3(2^k \pm 1)})$. In case Q_1 affords ρ^{-}, no two of the modules X_i are isomorphic (because $0, 3, 9, 21, 45$ and 93 all lie in different 2-cyclotomic cosets (mod 63) as defined before Lemma 5.4), so $ker\ \varphi^*$ contains all but one of the X_i and Corollary 5.3 applies.

Suppose that $Q_1 \otimes Q_2$ affords $\rho^{+} \otimes \rho^{+}$. Then $\lambda\mu(\kappa\phi)(\tau) = \lambda\mu(\kappa\phi)(1, \sigma_2^{3(2^k+1)})$ by Corollary 5.2.2. This action is reducible only if $gcd(1 + 2^k, 63) > 1$, in which case $k = 1, 3, 5$. Now $3(2^1 + 1) = 9$ and $3(2^5 + 1) \equiv 36 = 9 \cdot 4$ (mod 63) are in the same 2-cyclotomic coset (mod 63), but $3(2^3 + 1) = 27$ is not in this 2-cyclotomic coset (mod 63). It follows that $J = \{1, 5\}$. Now τ acts homocyclicly on $X_1 \oplus X_5$ as an element of order 7, and so the T-invariant subspaces are the 1-spaces of a 4-dimensional $GF(8)$-vector space X. It follows that $r = 8$. The element $\pi \in H$ acts on the $GF(8)$-projective space PX as a field automorphism. Consequently, the H-invariant submodules of X that might possibly be M are the 15 hyperplanes in PX that are invariant under π and defined over the prime field fixed by π.

Let $g \in G_{\{\alpha\beta\}} \setminus G^{+}$ be a 2-element interchanging α and β. Then g normalizes P and H, and interchanges Q_1 with Q_2, inducing an element of $N_{End(Q_1 \otimes Q_2)}(H)$. Moreover, $g^2 \in N_{\Gamma L(1,64)}(H)$, which has odd order. Thus we can choose g to be an involution. Since $N_{End(Q_1 \otimes Q_2)}(H)$ has twice odd order and contains a map interchanging Q_1 with Q_2, Sylow's theorem allows us to take g to be such a map. Now g interchanges X_1 with X_5, and there are but three g-invariant hyperplanes in PX. They fall in a single $\langle\omega\rangle$-orbit, so there is an essentially unique choice for M. It works. Formally, this is as follows:

Construction 5.7. *Let Q_1 and Q_2 be copies of $GF(64)$ and let $tr\colon GF(64) \to GF(8)$ be the usual trace map. Let $H = \langle \tau = \omega^3, \pi = \omega\sigma^2 \rangle \leqslant \Gamma L(1, 64) = \langle \omega, \sigma \mid \omega^{63} = \sigma^6 = 1, \omega^{\sigma} = \omega^2 \rangle$ act naturally on Q_1 and Q_2. Then the commutator form*

$$\varphi\colon Q_1 \times Q_2 \to GF(8) \qquad \text{given by } \varphi(x, y) = tr(xy^2 + x^2 y)$$

meets the conditions of Proposition 4.5 and is H-equivariant (for appropriate action of H on $GF(8)$). It therefore gives rise to a distance-transitive graph Γ. Any distance-transitive $8 \cdot K_{64,64}$ that is not isomorphic to $PG_3(8)^{op}$ is isomorphic to Γ.

6. The Affine Case

In this section we complete the proof of the Main Theorem in the affine case, $H^{(i)} \leqslant AGL(a, p)$, with Propositions 6.3, 6.4 and 6.6. In view of Lemma 4.6 and Corollary 4.7, we may assume that $p < r = p^b \leqslant k = p^a$ and $p^a \geqslant p^3$. Consequently, either $p^a = 2^6$ or there exists a primitive prime divisor t of $p^a - 1$, by [25]. Since G interchanges $H^{(1)}$ and $H^{(2)}$, these two permutation groups are isomorphic. By Lemma 2.2.1, this common type H_0 has order divisible by $p^a - 1$. Hence whenever a primitive prime divisor t of $p^a - 1$ exists, a Sylow t-subgroup T of $G_{\alpha\beta}$ is a cyclic Singer group.

Lemma 6.1. *Suppose that $T \leqslant G_{\alpha\beta}$ acts as a Singer cycle on Q_i, $i = 1, 2$, and acts trivially on K. Suppose in addition that whenever $T, T^g \leqslant H \leqslant N_G(G_{\alpha\beta})$, for $g \in G$, then there is $h \in H$ such that $T^{gh} = T$. Then the Main Theorem holds.*

Proof. Since Corollary 5.3 applies, the group $T = \langle\tau\rangle$ is cyclic, and Q_1 and Q_2 are contragredient T-modules. We remind the reader of the necessary notation. Recall that Schur's lemma and the irreducibility of T on Q_i has allowed us to identify the commuting ring $E_i = End_T(Q_i)$ to be $GF(p^a)$, $i = 1, 2$. The multiplicative group S_i of E_i is a cyclic Singer group on Q_i, $i = 1, 2$, and $T = \langle \tau \rangle$ may be regarded as a subgroup of $S_1 \times S_2$, since $[K, T] = 1$. Let τ_i be the projection of τ in S_i, $i = 1, 2$. We also have fixed $x_i \in Q_i$ and labelled the elements $e_i x_i \in Q_i$ with $e_i \in E_i$, $i = 1, 2$. In addition, we have fixed a field isomorphism $\phi: E_1 \to E_2$ and an (additive) abelian group homomorphism $\nu: E_2 \to K$ such that the bi-additive map φ that determines the commutator form of P as in Section 4 is given by $\varphi(e_1x_1, e_2x_2) = \nu(\phi(e_1)e_2)$, where $\phi(e_1)e_2$ denotes multiplication in E_2.

Suppose that Γ is a counterexample to the Main Theorem. Take $g \in G$ to interchange α and β. Then g interchanges Q_1 with Q_2. By the conjugacy assumption and the Frattini argument, g may be taken in $N_G(T)$. Now g acts on K and satisfies

$$\nu(\phi(g(x_1e_1))g(x_2e_2)) = g(\nu(\phi(e_1)e_2)) \qquad \text{for all } x_ie_i \in Q_i, \quad i = 1, 2,$$

by Proposition 4.5 and Corollary 5.3. Since Q_1 and Q_2 are contragredient T-modules, $\tau_1^g = \tau_2^{-\alpha}$, for some $\alpha \in Aut\,\mathscr{E}$.

Let M^+ be the group of all pairs (n_1, n_2) in the normalizer of T in $Aut\,Q_1 \times Aut\,Q_2$ for which there is an $n \in Aut\,K$ such that

$$\nu(\phi(n_1(x_1e_1))n_2(x_2e_2)) = n(\nu(\phi(e_1)e_2)) \qquad \text{for all } x_ie_i \in Q_i, \quad i = 1, 2,$$

and let $M = \langle g, M^+ \rangle$. By Lemma 2.2, $G_{\alpha\beta}$ acts transitively on $B \setminus \{\alpha\}$, where B is the antipodal block containing α and T fixes this set pointwise, so the conjugacy assumption and the Frattini argument again imply that the normalizer of T in $G_{\alpha\beta}$ acts transitively on $B \setminus \{\alpha\}$. It follows that $N_{G_{\alpha\beta}}(T)$ must act on E_2, leaving invariant the subgroup $ker\,\nu$ and acting transitively on the non-trivial elements of $E_2/ker\,\nu$. By Proposition 4.5 and the definition of M^+, M^+ is the image in $Aut\,Q_1 \times Aut\,Q_2$ of $N_{Aut\,G_{\alpha\beta}}(T)$.

Conversely, if $N_{Aut\,P}(Q_i)$ acts transitively on the non-trivial elements of Q_i, $i = 1, 2$, and $M \leqslant N_{Aut\,Q_1 \times Q_2}(T)$ satisfies the above conditions, then the coset geometry $K(P, Q_1, Q_2)$ is distance-transitive by Proposition 4.5.

For each $i = 1, 2$, the group $R_i = M \cap S_i$ acts homocyclicly on $P_i = Q_i \times K$ as shown in the proof of Lemma 4.6. Therefore the ring of R_i-endomorphisms on both the domain and range of ν is a finite field, say $GF(q)$, and ν is $GF(q)$-linear. The choice of M implies that R_i has order $q - 1$. If R_i, $i = 1$ or 2, acts transitively on $E_2/ker\,\nu$, then $q = p^b$ and Lemma 4.6 implies that case (1) of the Main Theorem holds. Otherwise, the required transitivity of M on $E_2/ker\,\nu$ forces $\bar{M} = M/(M \cap (S_1 \times S_2))$ to act transitively on the points of the $GF(q)$-projective space $\mathscr{P}$ supported by $E_2/ker\,\nu$.

For notational consistency with case (5) of the Main Theorem, redefine $b = dim_{GF(q)}\,Im(\nu)$, and $a = dim_{GF(q)}\,\mathscr{E}$. In order for M to act transitively on the non-trivial R_i-orbits in $E_2/ker\,\nu$, $(q^b - 1)/(q - 1)$ must divide the order of $\bar{M}$. More than this, the cyclic group $M^+/(M \cap (S_1 \times S_2))$ cannot have orbits of size $(q^b - 1)/2$ on the non-trivial elements of $E_2/ker(\nu)$ without acting as a Singer cycle and having a group of scalars of order $gcd(q^{b-1} + \ldots + 1, q - 1) = gcd(b, q - 1)$ acting trivially on the points of $\mathscr{P}$. Therefore $(q^b - 1)gcd(b, q - 1)$ divides $2a(q - 1)$. □

We formally record some of the graphs falling in case (5).

Construction 6.2. *Suppose that* $(q^b - 1)gcd(b, q - 1)$ *divides* $2a(q - 1)$, *where* q *is a power of the prime* p, *and let* $F = GF(q^a)$. *In the situation of Corollary 5.2, take* $A \leqslant N_{Aut\,Q_1 \otimes Q_2}(\lambda\mu\mathscr{E})$ *to be an abelian group of order* $gcd(b, q - 1)(q^b - 1)/(q - 1)$ *that interchanges* Q_1 *with* Q_2 *and for which* $C_{A^+}(\lambda\mu\mathscr{E}) = 1$, *where* $A^+ = N_A(Q_1)$. *Let* B *be a* *normal basis for the field E_2 over $GF(q)$ so that $A \cap diag\, Aut\, E_2$ acts semi-regularly on* B. *Let W be a minimal A-invariant $GF(q)$-subspace containing an element of* B.

There are three possible A-module structures for W, namely: (*a*) *W is of dimension $|A|$ and a free A-module;* (*b*) *W is of dimension $|A^+|$ and the* (*unique*) *trivial A^+-submodule affords the trivial character of A;* (*c*) *W is of dimension $|A^+|$ and the* (*unique*) *trivial A^+-submodule affords the alternating character, sgn of A.*

In the first two cases take K to be a faithful irreducible submodule of W and in the third take K to be a faithful irreducible submodule of $sgn \otimes W$. Then there is an A—invarint map $\nu: E \to K$, which in turn determines a totally surjective map φ^* as in Corollary 5.3.

Since W affords a multiple of the regular representation of A, every $GF(q)A^+$-irreducible module actually occurs within W. The arithmetic condition $(q^b - 1)gcd(b, q-1) \mid 2a(q-1)$ ensures that A^+ has at most two orbits on the points of the $GF(q)$-projective space supported by $E/ker\, \nu$ and these are fused by the cyclic group A. Thus there exists a map φ meeting all of the criteria set in Proposition 4.5, *and so distance-transitive graphs Γ of this type exist.*

The first instance of this construction occurs with $p^a = 8$ and $p^b = 4$, and appears in [16]. The complete enumeration of this surely large class of graphs could be difficult.

Proposition 6.3. *Suppose that $p^a \neq 2^6$. Then the Main Theorem holds unless T acts non-trivially on K and $a = b$.*

Proof. Suppose that $p^a \neq 2^6$, t_0 is a primitive prime divisor of $p^a - 1$ and T is a Sylow t_0-subgroup of $G_{\alpha\beta}$. Then T can act non-trivially on K only if $a = b$, because otherwise t_0 does not divide $|Aut\, K|$, since t_0 is a primitive prime divisor of $p^a - 1$. As mentioned at the beginning of Section 5, T acts as a Singer cycle on Q_i, $i = 1, 2$, so the result follows from Sylow's theorem and Lemma 6.1. □

Proposition 6.4. *The Main Theorem holds when $p^a = 2^6$ unless $b = 6$ and $H \leq \Gamma L(1, 64)$ contains T acting as a cyclic Singer group on Q_i, $i = 1, 2$.*

Proof. Suppose not and that G, acting on Γ, is a counterexample. The affine 2-transitive groups have been classified by Liebeck, who credits Hering [18, Appendix]. It is a simple matter to go through the list of 2-transitive groups of degree 2^6 looking for possible Singer cycles of order, say, t, satisfying the conjugacy assumptions of Lemma 6.1. Since $b \neq 1$ the group $G_2(2)'$ need not be considered and $SL(2, 8) \leq Sp(6, 2)$, so we arrive at only three cases: (a) $SL(2, 8) \leq H_0$, $t = 9$; (b) $SL(3, 4) \leq H_0$, $t = 9$; and (c) $H_0 \leq \Gamma L(1, 64)$, for $t = 21$. In the first two cases the conjugacy result assumed in Lemma 6.1 is well known and appears in, for example, [7, pp. 6 and 24], and in the third it is immediate, since $\Gamma L(1, 64)$ has but one cyclic subgroup of order 21.

The full inverse image $T \leq G_{\alpha\beta}$ of such a Singer cycle acts non-trivially on K by Lemma 6.1. But this forces $H \leq H_0 \times H_0$ to act non-trivially on K as well. In cases (a) and (b) the only non-trivial representations of H_0 on a vector space of a cardinality dividing 2^6 are the natural module and its contragredient, and the known decomposition of the tensor product of these modules has no non-trivial homomorphic image of cardinality ≤ 64 [18, Theorem 2.2]. Therefore $H_0 \leq \Gamma L(1, 64)$, and $t = 21$. It follows that $b = 2$, 3 or 6.

If $b \neq 6$, then either the discussion leading to Construction 5.7 applies or T may be taken to be cyclic of order 63. If $b = 2$ ($b = 3$), the kernel of the action of T on K has order 21 (9) and Lemma 5.3 and the proof of Lemma 6.1 implies that case (1) of the Main theorem holds. □

Although the case $a=b$ has already appeared [21], we take this opportunity to sharpen that result by showing that no proper generalized twisted fields give rise to distance-transitive graphs. The discussion near the end of Section 5 fills a small gap at the end of the argument in [21] and strengthens a theorem of Dempwolff [11].

THEOREM 6.5. *Suppose that a projective plane in Lenz class V of order p^a admits a cyclic group that leaves invariant two affine lines on each of which it has at least one point orbit of length $(p^a-1)/gcd(p^a-1, a)$. Then the plane is a generalized twisted field plane.*

PROOF. Since Kleinfeld has shown that there are exactly two projective planes of order 16 in Lenz class V and neither admits an automorphism of order 15, cf. [10, p. 242], this follows from Lemma 5.4. □

The proof of the Main Theorem has been reduced to the case $a=b$, and all that remains is to show that only twisted fields can arise in case (5) of the Main Theorem.

PROPOSITION 6.6. *The only generalized twisted fields that give rise to distance-transitive covers of complete bipartite graphs are the twisted fields.*

PROOF. By Lemma 3.3 of [21], $G_{\alpha\beta}\leqslant \Gamma L(1,p^a)\times\Gamma L(1,p^a)$ and it follows that $G_{\{\alpha\beta\}}$ contains a cyclic normal subgroup $T=\langle\tau\rangle$ of order $t=(p^a-1)/d$, where d is the greatest common divisor of p^a-1 and a. Take $g\in G_{\{\alpha,\beta\}}$, interchanging α and β. Since g normalizes T it induces a ring isomorphism $\phi\colon End_T(Q_1)\to End_T(Q_2)$. By using this map for ϕ in Corollary 5.2, we may take $x=y=d$ in Corollary 5.2.2.

Let X_i and J be as in the discussion before Lemma 5.4. This choice for ϕ only allows us to conclude from Lemma 5.4 that $\varphi^*\in X_i\oplus X_j\leqslant Q_1\otimes Q_2$ for some $0\leqslant i\neq j<a$. The fact that X_i and X_j must be isomorphic T-modules implies that $1+p^i$ and $1+p^j$ are in the same p-cyclotomic coset $(\mathrm{mod}\, t)$ and we are led to study solutions to the congruences

$$p^{a_1}+p^{a_2}\equiv p^{b_1}+p^{b_2}\quad (mod\, t)\qquad \text{where } a_1-a_2\not\equiv b_1-b_2\quad (mod\, a). \tag{3}$$

It is sufficient to show that there is a matching of exponents. The methods of the proof of Lemma 5.5 apply. Because the result is immediate wheh the congruence is equality, we ask: When might the sum of two powers of p be greater than t? The normalization in the second paragraph of the proof of Lemma 5.5 leads to the inequalities:

$$d(1+p)\geqslant p^{1+\lceil a/4\rceil}\qquad\text{and}\qquad 2d\geqslant p^{\lceil a/3\rceil},$$

which only have solutions when $p^a\in\{2^6, 3^4, 3^8\}$. Direct examination of these cases show that the congruences (3) have no solutions. □

ACKNOWLEDGEMENTS

A. A. Ivanov wishes to thank the University of Western Australia for its hospitality while part of this work was done. Robert A. Liebler's research was partially supported by NSA grant 904-91-H-0048. Cheryl E. Praeger's research was supported by ARC grant A68931532.

We thank A. Brouwer for interest, encouragement and helpful conversations. We also thank D. V. Pasechnik and his computer for announcing the first complete uniqueness proof of the graphs in case 6 of the Main Theorem. Finally, we thank the referee for numerous helpful suggestions.

References

1. A. A. Albert, Isotopy for generalized twisted fields, *Anais Academia Brasileir de Ciencias,* **33** (1961), 265–275.
2. J. T. M. van Bon and A. E. Brouwer, The distance-regular antiposal covers of classical distance-regular graphs, *Colloq. Math. Janos Bolyai, Proc. Eger 1987* (1988), 141–166.
3. A. E. Brouwer, A. M. Cohen and A. Neumaier, *Distance Regular Graphs,* Springer-Verlag, Berlin, 1989.
4. W. Burnside, *Theory of Groups of Finite Order* (2nd edn), Cambridge University Press, London, 1911 (reprinted Chelsea, New York, 1958).
5. P. J. Cameron, Finite permutation groups and finite simple groups, *Bull. Lond. Math. Soc.,* **13** (1981), 1–22.
6. I. V. Chuvaeva and D. V. Pasechnik, Distance-transtive graphs of type $q \cdot K_{q,q}$ and projective planes, *Europ. J. Combin.,* **11** (1990), 341–346.
7. J. H. Conway, R. T. Curtis, S. P. Norton, R. P. Parker and R. A. Wilson, *Atlas of Finite Groups,* Clarendon Press, Oxford, 1985.
8. A. Cronheim, T-groups and their geometry, *Illinois J. Math.,* **9** (1965), 1–30.
9. C. W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras,* John Wiley, New York, 1966.
10. P. Dembowski, *Finite Geometries,* Springer-Verlag, New York, 1968.
11. U. Dempwolff, A characterization of generalized twisted field planes, *Arc. Math.,* **50** (1988), 477–481.
12. I. A. Faradzev, A. A. Ivanov and A. V. Ivanov, Distance-transitive graphs of valencies 5, 6 and 7, *Europ. J. Combin.,* **7** (1986), 303–319.
13. A. Gardiner, Antipodal covering graphs, *J. Combin. Theory, Ser. B,* **16** (1974), 255–273.
14. A. Gardiner, Imprimitive distance-regular graphs and projective planes, *J. Combin. Theory, Ser. B,* **16** (1974), 274–281.
15. A. Gardiner and C. E. Praeger, Distance-transitive graphs of valency six, *Proc. Edinb. Math. Soc.* (2), **30** (1987), 73–81.
16. A. A. Ivanov and A. V. Ivanov, Distance-transitive graphs of valency k, $8 \leqslant k \leqslant 13$, in: *Algebraic, Extremal and Metric Combinatorics,* Cambridge University Press, Cambridge, 1988, pp. 112–145.
17. M. J. Kallaher, A survey of weak rank 3 affine planes, In: *Proceedings of the International Conference on Projective Planes,* Washington State University Press, Pullman (1973), pp. 121–141.
18. M. W. Liebeck, The affine permutation groups of rank three, *Proc. Lond. Math. Soc.* (3), **54** (1987), 477–516.
19. R. A. Liebler, Finite affine planes of rank 3 are translation planes, *Math. Z.,* **116** (1970), 89–93.
20. R. A. Liebler, On nonsingular tensors and related projective planes, *Geom. Ded.,* **11** (1981), 455–464.
21. R. A. Liebler, The classificaton of distance-transitive graphs of type $q \cdot K_{q,q}$, *Europ. J. Combin.,* **12** (1991), 125–128.
22. C. E. Praeger, The inclusion problem for finite primitive permutation groups, *Proc. Lond. Math. Soc.* (3), **60** (1990), 68–88.
23. D. H. Smith, Primitive and imprimitive graphs, *Q. J. Math. Oxford* (2), **6** (1973), 659–662.
24. J. A. Todd, On representations of the Mathieu groups as collineation groups, *J. Lond. Math. Soc.,* **34** (1959), 406–416.
25. K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math. Phys.,* **3** (1892), 265–284.

Received 18 *August* 1993 *and accepted in revised form* 15 *January* 1996

A. A. Ivanov
Department of Mathematics,
Imperial College,
180 Queen's Gate,
London SW7 2BZ, U.K.

Robert A. Liebler
Department of Mathematics,
Colorado State University,
Fort Collins, Colorado 80524, U.S.A.

and

Tim Penttila and Cheryl E. Praeger
Department of Mathematics,
University of Western Australia,
Perth, W.A. 6907, Australia